

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000032056 A**(43) Date of publication of application: **28.01.00**

(51) Int. Cl.

**H04L 12/56**  
**H04L 12/46**  
**H04L 12/28**  
**H04L 12/66**

(21) Application number: **10210387**(22) Date of filing: **09.07.98**(71) Applicant: **NEC CORP**

(72) Inventor: **YAMADA KENSHIN**  
**SERA TAKAFUMI**  
**ARUTAKI AKIRA**

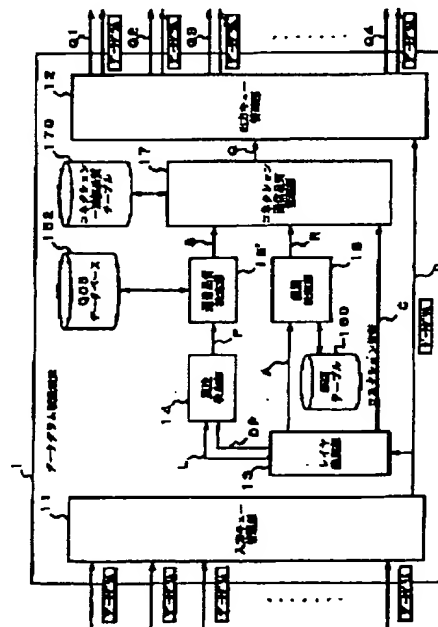
(54) **COMMUNICATION QUALITY CONTROLLER**

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide the communication quality controller that decides optimum communication quality from a received datagram and transfers it.

**SOLUTION:** An attribute detection section 14 extracts attribute information of communication from information of a protocol layer or any layer and a communication quality decision section 15 and a connection communication quality management section 17 decides the communication quality for the transmission of the datagram according to quality information of connection corresponding to the extracted attribute information in addition to decision of a destination by data below the protocol layer included in the datagram.

COPYRIGHT: (C)2000,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-32056

(P2000-32056A)

(43) 公開日 平成12年1月28日 (2000.1.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	キーワード(参考)
H 0 4 L	12/56	H 0 4 L 11/20	1 0 2 D 5 K 0 3 0
	12/46	11/00	3 1 0 C 5 K 0 3 3
	12/28	11/20	B
	12/66		

審査請求 有 請求項の数28 F D (全 29 頁)

(21) 出願番号 特願平10-210387

(22) 出願日 平成10年7月9日 (1998.7.9)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 山田 肇吾

東京都港区芝五丁目7番1号 日本電気株式会社内

(72) 発明者 世良 孝文

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100093595

弁護士 松本 正夫

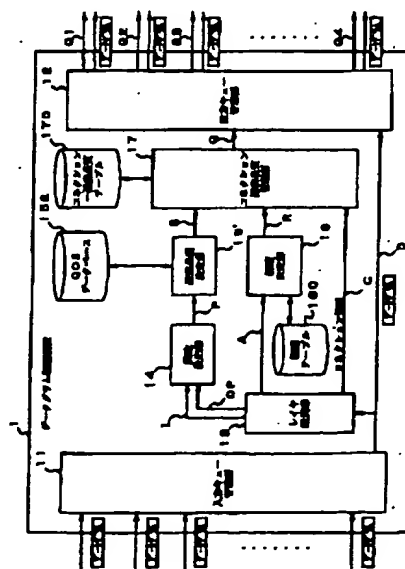
最終頁に続く

(54) 【発明の名称】 通信品質制御装置

(57) 【要約】

【課題】 受信したデータグラムにおいて、最適な通信品質を決定しデータグラムを転送する通信品質制御装置を提供する。

【解決手段】 データグラムに含まれるプロトコルレイヤ3以下のデータにより送信先を決定するだけでなく、プロトコルレイヤ、4、5、6、7の各々またはいずれかのレイヤの情報より通信の属性情報を属性検出部14により取り出し、取り出した属性情報に対応する接続の品質情報にしたがって通信品質決定部15及び接続通信品質管理部17にてデータグラムを送信する通信品質を決定する。



(2)

特開2000- 32056

2

## 【特許請求の範囲】

1  
【請求項1】 既存データネットワークのプロトコルレイヤを終端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を終端するプロトコル終端装置と、プロトコルレイヤ3以下の通信の属性とこれら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に対応するコネクションの品質情報に従って指定された終端装置に対して前記データグラムを転送する通信データグラム転送装置とを有し、通信の属性に対応するコネクションの品質に最適なデータグラム転送機能を実現する通信品質制御装置において、前記通信データグラム転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ3以下のレイヤの情報に含まれる識別情報を検査すると同時にデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し各々のプロトコルレイヤの通信の属性情報を取り出す属性識別手段と、前記データグラムがプロトコル終端装置で受信された場合に前記データグラムから導出された各々のプロトコルレイヤの通信の属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質を決定し、前記プロトコル終端装置に対して通知する通信品質決定手段とを備えることを特徴とする通信品質制御装置。

【請求項2】 既存データネットワークのプロトコルレイヤを終端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を終端するプロトコル終端装置と、これら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に対応するコネクションの品質情報に従って指定された終端装置に対して前記データグラムを転送する通信データグラム転送装置とを有し、通信の属性に対応するコネクションの品質に最適なデータグラム転送機能を実現する通信品質制御装置において、前記通信データグラム転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し各々のプロトコルレイヤの通信の属性情報を取り出す属性識別手段と、前記データグラムがプロトコル終端装置で受信された場合に前記データグラムから導出された各々のプロトコルレイヤの通信の属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質を決定し、前記プロトコル終端装置に対して通知する通信品質決定手段とを備えることを特徴とする通信品質

制御装置。

【請求項3】 前記属性識別手段が、

受信されたデータグラムより、前記レイヤ情報を識別すると共に、前記データグラムのコネクション識別情報よりコネクションの状態を識別してコネクション情報として前記通信品質決定手段に出力し、かつ前記データグラムの転送経路を決定し転送先経路情報として前記通信品質決定手段に出力し、

前記通信品質決定手段は、前記属性情報に対応するコネクションの品質情報を決定し、前記コネクション情報と、前記コネクションの品質情報と、前記転送先経路情報により、データグラムを送信する通信品質を決定することを特徴とする請求項1または請求項2に記載の通信品質制御装置。

【請求項4】 前記属性識別手段は、識別したコネクションの状態から、レイヤ4以上の属性を検出する必要があると判断した場合に、前記レイヤ情報と、前記データグラムの一部または全部に基づいて、通信の属性情報を取り出すことを特徴とする請求項3に記載の通信品質制御装置。

【請求項5】 前記通信データグラム転送装置が、コネクション情報と通信品質を組にして記録したコネクションー通信品質テーブルを備え、

前記通信品質決定手段は、前記コネクション情報と前記転送先経路情報、またはコネクション品質情報が入力した場合に、前記データグラムが前記コネクションー通信品質テーブルによる管理が必要かどうかを判断し、

管理の必要がある場合、前記コネクションー通信品質テーブルに同一のコネクションが存在するかを検索し、同一のコネクションが存在する場合、コネクションー通信品質テーブルを参照して通信品質を決定し、存在しない場合、前記コネクション情報と、前記コネクションの品質情報と、前記転送先経路情報により通信品質を決定し、かつコネクション情報と通信品質を組にして前記コネクションー通信品質テーブルに記録し、管理の必要がない場合、前記コネクション情報と前記転送先経路情報により通信品質を決定することを特徴とする請求項3または請求項4に記載の通信品質制御装置。

【請求項6】 前記属性情報に対応する前記コネクション品質情報を格納するデータベースを備え、前記通信品質決定手段は、前記データベースを参照し、前記属性情報に基づいて前記コネクション品質情報を決定することを特徴とする請求項1乃至請求項5に記載の通信品質制御装置。

【請求項7】 レイヤ3をIPとし、レイヤ4をTCPとし、レイヤ5をHTTPとし、前記属性識別手段は、

前記データグラムのIPヘッダのプロトコル番号、または該プロトコル番号と前記データグラムのTCPプロト

(3)

特開2000- 32056

3

4

コルヘッダ内のポートアドレス、または前記データグラムのIPヘッダの次ヘッダ値、または該次ヘッダ値と前記データグラムのTCPプロトコルヘッダ内のポートアドレスとを检查し、レイヤ5がHTTPであることを認識するとともに受信データグラムのTCPヘッダまたは、TCPヘッダ及びHTTPメッセージに含まれる一つまたは複数の識別情報を检查し、

前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項8】 前記属性識別手段が、

前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent typeによりデータグラムのメディア属性、HTTPヘッダに含まれるFromフィールドによりデータグラムを送出したユーザの電子メールアドレス、HTTPヘッダに含まれるUser-Agentによりデータグラムを作成したユーザプログラム名及びVersion、HTTPヘッダに含まれるServerによりデータグラムを作成したサーバソフトウェア名及びVersionの少なくとも1を检查することを特徴とする請求項7に記載の通信品質制御装置。

【請求項9】 前記属性識別手段が、

前記識別情報として、受信データグラムのHTTPヘッダに含まれるDateによりデータグラムの作成日時、HTTPヘッダに含まれるAuthorizationによりデータグラムの認証情報、当該認証情報の暗号化方法、HTTPヘッダに含まれるExpiresによりデータグラムの有効日時の少なくとも1を检查することを特徴とする請求項7に記載の通信品質制御装置。

【請求項10】 前記属性識別手段が、

前記識別情報として、受信データグラムのHTTPヘッダに含まれるPragmaによりデータグラムの要求事項、HTTPヘッダに含まれるCache-Controlによりデータグラムのキャッシュ制御情報、HTTPヘッダに含まれるIf-Modified-SinceによりMethodの実行条件、HTTPヘッダに含まれるIf-Unmodified-SinceによりMethodの実行条件、HTTPヘッダに含まれるリクエスト行(Request-Line)内のリクエストURIによりクライアントの要求しているURI、HTTPヘッダに含まれるLast-ModifiedによりHTTPデータの最終更新日時の少なくとも1を检查することを特徴とする請求項7に記載の通信品質制御装置。

【請求項11】 前記属性識別手段が、

前記識別情報として、受信データグラムのHTTPヘッダに含まれるRefererによりHTTPデータの参照元URI (Uniform Resource Identifiers)、HTTPヘッダに含まれるLocationによりHTTPデータのおかれているURI、HTTPヘッダに含まれるForwardedによりデータグラムの転送先URI及び転送元ドメインネーム、HTTPヘッダに含まれるContent-BaseによりデータグラムのbaseURI、HTTPヘッダに含まれるContent-LocationによりHTTPデータの存在するURI、HTTPヘッダに含まれるMethodによりユーザプログラムからのHTTPデータ要求方法の少なくとも1を检查することを特徴とする請求項7に記載の通信品質制御装置。

【請求項12】 前記属性識別手段が、

前記識別情報として、受信データグラムのHTTPヘッダに含まれるMIME-VersionによりデータグラムがMIME (Multipurpose Internet Mail Extensions)のVersion、HTTPヘッダに含まれるAcceptによりユーザプログラムの許可するメディア属性、HTTPヘッダに含まれるAccept-Charsetによりユーザプログラムの許可する文字セット、HTTPヘッダに含まれるAccept-Encodingによりユーザプログラムの許可するデータグラムのコーディング方法、HTTPヘッダに含まれるAccept-Languageによりユーザプログラムの許可するデータグラムの言語、HTTPヘッダに含まれるContent-Encodingによりデータグラムのエンコード方法、HTTPヘッダに含まれるContent-Languageによりデータグラムの言語の少なくとも1を检查することを特徴とする請求項7に記載の通信品質制御装置。

【請求項13】 前記属性識別手段が、

前記識別情報として、受信データグラムのHTTPヘッダに含まれるStatus Codeによりユーザプログラムからの要求に対するサーバの応答内容、HTTPヘッダに含まれるWWW-Authenticateによりサーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authenticateによりプロキシ・サーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authorizationによりデータグラムの認証情報の少なくとも1を检查することを特徴とする請求項7に記載の通信品質制御装置。

【請求項14】 前記属性識別手段が、

前記識別情報として、受信データグラムのHTTPヘッダに含まれるAllowによりHTTPデータの許可するMethod、HTTPヘッダに含まれるAccept-Rangeによりサーバの許可するRange要求

50

(4)

特開2000- 32056

5

方法、HTTPヘッダに含まれるHostによりHTTPデータを要求されるホスト及びそのポート番号、HTTPヘッダに含まれるIf-RangeによりHTTPデータの取得条件、HTTPヘッダに含まれるPublicによりサーバの許可するMethod、HTTPヘッダに含まれるRangeによりユーザプログラムの要求しているHTTPデータのRangeの少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項15】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent-Lengthによりデータグラムのデータ長、HTTPヘッダに含まれるConnectionによりデータグラムのコネクションの状態、HTTPヘッダに含まれるWarningによりユーザプログラムの要求に対するサーバの応答情報、HTTPヘッダに含まれるRetry-Afterにより要求されたHTTPデータを取得可能な日時、HTTPヘッダに含まれるViaによりパケットを中継してきたプロキシサーバまたはゲートウェイのプロトコルVersion及びホスト名及び使用ソフトウェア名、HTTPヘッダに含まれるTransfer-Encodingによりデータグラムのコーディング方法の少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項16】 レイヤ3をIPとし、レイヤ4をTCPまたはUDP (User Datagram Protocol) として、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号またはIPヘッダの次ヘッダ値を検査し、レイヤ4がTCPまたはUDPであることを認識するとともに、識別情報として受信データのTCPヘッダまたはUDPヘッダに含まれる一つまたは複数の識別情報を検査し、前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項17】 前記属性識別手段は、前記識別情報として、受信データグラムのUDPヘッダに含まれるchecksumフィールドを検査することを特徴とする請求項16に記載の通信品質制御装置。

【請求項18】 レイヤ3をIPとし、レイヤ4をTCPまたはUDPとし、レイヤ5をDNSまたはTFTPまたはSNMPとして、前記属性識別手段は、前記データグラムのIPヘッダの

6

プロトコル番号、または該プロトコル番号と前記データグラムのTCPまたはUDPプロトコルヘッダ内のポートアドレス、または前記データグラムのIPヘッダの次ヘッダ値、または該ヘッダ値と前記データグラムのTCPまたはUDPプロトコルヘッダ内のポートアドレスを検査し、レイヤ5がDNSまたはTFTPまたはSNMPであることを認識するとともに、識別情報として受信データのDNSメッセージ、TCPまたはUDPヘッダとDNSメッセージ、TFTPメッセージ、UDPヘッダとTFTPメッセージ、SNMPメッセージ、またはUDPヘッダとSNMPメッセージの何れかに含まれる一つまたは複数の識別情報を検査し、

前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項19】 前記属性識別手段は、前記識別情報として、受信データグラムのDNSメッセージにquery typeが存在するかどうかを検査することを特徴とする請求項18に記載の通信品質制御装置。

【請求項20】 前記属性識別手段は、前記識別情報として、受信データグラムのTFTPメッセージに含まれるopcodeを検査することを特徴とする請求項18に記載の通信品質制御装置。

【請求項21】 前記属性識別手段は、前記識別情報として、受信データグラムのSNMPメッセージに含まれるPDUタイプを検査することを特徴とする請求項18に記載の通信品質制御装置。

【請求項22】 レイヤ3をIPとし、レイヤ4をTCPとし、レイヤ5をFTPまたはSMTPまたはとして、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号、または該プロトコル番号と前記データグラムのTCPプロトコルヘッダ内のポートアドレス、または前記データグラムのIPヘッダの次ヘッダ値、または該ヘッダ値と前記データグラムのTCPプロトコルヘッダ内のポートアドレスを検査し、レイヤ5がFTPまたはSMTPであることを認識するとともに、識別情報として受信データのFTP Command、FTP Reply、TCPヘッダとFTP CommandまたはFTP Reply、SMTP Command、SMTP Reply Code、SMTPヘッダ、TCPヘッダとSMTP CommandまたはSMTP Reply CodeまたはSMTPヘッダの何れかに含まれる一つまたは複数の識別情報を検査し、

前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクシオンに最適なレイヤ3以下のコネクシオンの品質を決定し、コネクシオンの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクシオン品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項23】 転送の物理レイヤをATM転送方式とし、コネクシオン品質に基づきデータグラム転送処理としてATMの各々のコネクシオン品質に別々のVC (Virtual Circuit) を割り当ててデータグラムの転送を行ない、各々のVCはコネクシオン品質に応じた通信品質制御パラメータが設定されていることにより、データグラムから導出されるメディアの属性に応じた転送が行なわれることを特徴とする請求項1乃至請求項22に記載の通品質制御装置。

【請求項24】 前記通信品質決定手段は、前記通信品質に加えて、コネクシオン設定のためのコネクシオン設定メッセージに応じてコネクシオン設定ロバストネスを選択して設定することを特徴とする請求項1乃至請求項23に記載の通品質制御装置。

【請求項25】 前記通信品質決定手段は、前記属性情報により、前記コネクシオンの通信品質として、最適な帯域幅に関する制御パラメータ、最大遅延時間や遅延時間変動量を含む遅延時間に関する最適な制御パラメータ、バッファ量を含むデータ喪失に関する最適な制御パラメータ、最適な課金情報に関する制御パラメータ、最適なセキュリティ品質に関する制御パラメータのうちの少なくとも1の制御パラメータを決定することを特徴とする請求項1乃至請求項24に記載の通品質制御装置。

【請求項26】 前記通信品質決定手段は、前記コネクシオンの通信品質に基づき、最適なデータグラムの転送先、最適なデータグラムの転送経路の少なくとも一方を決定することを特徴とする請求項1乃至請求項25に記載の通品質制御装置。

【請求項27】 前記通信品質決定手段は、前記コネクシオンの通信品質に基づいて、必要に応じて専用の物理回線を該コネクシオンによって使用し、前記データグラムを暗号化または復号化して転送し、データグラム内の不要な情報を削除し、圧縮によりデータグラムのサイズを削減し、データグラムのトンネリングを行なうことを特徴とする請求項1乃至請求項26に記載の通品質制御装置。

【請求項28】 前記通信品質決定手段は、前記属性情報によりコネクシオンの通信品質としてコネクシオン設定優先度またはコネクシオン転送優先度を設定し、該コネクシオン設定優先度の高いコネクシオンのコネクシオン設定処理を優先し、またはコネクシオン転

送優先度の高いコネクシオンのデータグラムの転送を優先させることを特徴とする請求項請求項1乃至請求項27に記載の通品質制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークの通信装置に関し、特にデータグラムの転送網上で既存データネットワークに位置する通信品質制御装置に関する。

【0002】

10 【従来の技術】 従来の通信網においては、例えばLAN (Local Area Network) では、Ethernet技術、ATM技術などの物理転送技術を基に上位プロトコルであるIP、さらにTCPによってデータグラムの転送を行なっている。

【0003】 また、LANのIPサブネット間を接続したインターネット (The Internet) においても、前述のEthernet技術やATM技術を始めとする各種物理転送方法が検討され装置に実装されている。

20 【0004】 もともとこれらのネットワークでは、エンドーエンド間における通信すなわちコネクシオンを保証するためのしくみであって、通信網内に位置するデータグラム中継転送する装置は、エンドーエンドの転送品質を満足するためには、あらかじめエンドーエンドのプロトコルの物理転送レイヤに指示された通信品質を各装置が満足するように転送機能を実現するように構成されている。

30 【0005】 さてこうした既存の通信網では、特にIPなどのレイヤ3の転送が重要視されておりルータ装置と呼ばれるIPレイヤを重点的に転送処理できる装置が網内に数多く配置されている。

【0006】 これらルータ装置ではレイヤ3のIPを終端し、そのデータグラムから導出される宛先IPアドレスから装置内にあらかじめ蓄積された経路情報から転送すべき経路を決定することによりデータグラムの転送を行なっている。この際、データグラムが送出される物理レイヤの処理は経路から容易に導き出される1経路を選択しデータグラムを該インタフェースから転送する処理を行なっている。

40 【0007】 なお、アプリケーションごとの通信品質を保証し、かつルータを用いることなく異なるサブネット間でデータ転送を可能とするネットワークサーバが、特開平9-116560号公報に開示されている。

【0008】

【発明が解決しようとする課題】 上述した従来のルータ装置では、データグラムの通信属性に応じたコネクシオン品質により最適な通信品質を決定しデータグラムを転送することができない。その理由は、データグラムから導出される宛先IPアドレスから装置内にあらかじめ蓄積された経路情報から転送すべき経路を決定することに

よりデータグラムを転送しているからである。

【0009】より具体的には、以下のような問題点があった。

【0010】第1に、動画、音声、画像などの通信属性に基づいて、最適な通信品質でデータグラムの転送ができない。

【0011】第2に、特定のユーザや団体の使用するトラフィックに対してある通信品質を提供する場合、IPアドレス等の宛先アドレス、送信元アドレスを用いてのみにしか、特定のユーザや団体を特定することができない。

【0012】第3に、通信属性により定まるコネクションの品質に応じた課金を行なうことができない。

【0013】第4に、データグラムがセキュリティ上非常に重要な情報を含んでいるかどうかを判別できないため、セキュリティ上重要な情報を含んだデータグラムと、そうでないデータグラムを同様の通信品質でデータグラム転送処理を行なってしまうため、セキュリティ品質に応じたデータグラム転送を実現することができない。

【0014】第5に、データグラムの新規性により、コネクション品質を決定することができない。

【0015】第6に、トランスポート層において規定されるコネクションにおいて、該コネクションの状態を判断し、該コネクションの通信品質を動的に変更することができない。

【0016】本発明の目的は、高速なレイヤ3以下のデータグラム転送機能を実現しながら、データグラムの通信の属性を認識し、抜き出された通信属性に最適な通信品質によりデータグラムを転送することを可能とする通信品質制御装置を提供することにある。

【0017】本発明の他の目的は、あらかじめ登録してあるユーザに対して高度かつ多様な通信サービスを実現でき、また、通信品質に応じた課金量で課金を行なうことができる通信品質制御装置を提供することにある。

【0018】本発明の他の目的は、データグラムがセキュリティ上非常に重要なデータを含んでいるかどうかを判断し、データグラムに対応するセキュリティ品質に応じたデータ転送を実現できる通信品質制御装置を提供することにある。

【0019】本発明の他の目的は、データグラムの新規性を判断し、コネクションの品質を決定することができ、また、同一のコネクションで認識できる情報だけでなく、他のコネクションにおいて認識した情報を基にコネクション品質を決定し、最適な通信品質でデータグラムを転送可能である通信品質制御装置を提供することにある。

【0020】

【課題を解決するための手段】上記目的を達成する本発明は、既存データネットワークのプロトコルレイヤを終

端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を終端するプロトコル終端装置と、プロトコルレイヤ3以下の通信の属性とこれら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に対応するコネクションの品質情報に従って指定された終端装置に対して前記データグラムを転送する通信データグラム転送装置とを有し、通信の属性に対応するコネクションの品質に最適なデータグラム転送機能を実現する通信品質制御装置において、前記通信データグラム転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ3以下のレイヤの情報に含まれる識別情報を検査すると同時にデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し各々のプロトコルレイヤの通信の属性情報を取り出す属性識別手段と、前記データグラムがプロトコル終端装置で受信された場合に前記データグラムから導出された各々のプロトコルレイヤの通信の属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質を決定し、前記プロトコル終端装置に対して通知する通信品質決定手段とを備えることを特徴とする。

【0021】また、請求項2の本発明は、既存データネットワークのプロトコルレイヤを終端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を終端するプロトコル終端装置と、これら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に対応するコネクションの品質情報に従って指定された終端装置に対して前記データグラムを転送する通信データグラム転送装置とを有し、通信の属性に対応するコネクションの品質に最適なデータグラム転送機能を実現する通信品質制御装置において、前記通信データグラム転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し各々のプロトコルレイヤの通信の属性情報を取り出す属性識別手段と、前記データグラムがプロトコル終端装置で受信された場合に前記データグラムから導出された各々のプロトコルレイヤの通信の属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質を決定し、前記プロトコル終端装置に対して通知する通信品質決定手段とを備えることを特徴とする。

【0022】このように、データグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し、各々プロトコルレイヤの通信情報を取り出すことにより、より厳密に通信の属性を特定することができ、該通信の属性に最適なコネ



(7)

特開2000- 32056

11

12

ション品質を用いてデータグラムの転送が可能となるものである。

【0023】請求項3の本発明の通信品質制御装置では、前記属性識別手段が、受信されたデータグラムより、前記レイヤ情報を識別すると共に、前記データグラムのコネクション識別情報よりコネクションの状態を識別してコネクション情報として前記通信品質決定手段に出力し、かつ前記データグラムの転送経路を決定し転送先経路情報として前記通信品質決定手段に出力し、前記通信品質決定手段は、前記属性情報に対応するコネクションの品質情報を決定し、前記コネクション情報と、前記コネクションの品質情報と、前記転送先経路情報により、データグラムを送信する通信品質を決定することを特徴とする。

【0024】請求項4の本発明の通信品質制御装置では、前記属性識別手段は、識別したコネクションの状態から、レイヤ4以上の属性を検出する必要があると判断した場合に、前記レイヤ情報と、前記データグラムの一部または全部に基づいて、通信の属性情報を取り出すことを特徴とする。

【0025】請求項5の本発明の通信品質制御装置では、前記通信データグラム転送装置が、コネクション情報と通信品質を組にして記録したコネクションー通信品質テーブルを備え、前記通信品質決定手段は、前記コネクション情報と前記転送先経路情報、またはコネクション品質情報が入力した場合に、前記データグラムが前記コネクションー通信品質テーブルによる管理が必要かどうかを判断し、管理の必要がある場合、前記コネクションー通信品質テーブルに同一のコネクションが存在するかを検索し、同一のコネクションが存在する場合、コネクションー通信品質テーブルを参照して通信品質を決定し、存在しない場合、前記コネクション情報と、前記コネクションの品質情報と、前記転送先経路情報により通信品質を決定しかつコネクション情報と通信品質を組にして前記コネクションー通信品質テーブルに記録し、管理の必要がない場合、前記コネクション情報と前記転送先経路情報により通信品質を決定することを特徴とする。

【0026】請求項6の本発明の通信品質制御装置では、前記属性情報に対応する前記コネクション品質情報を格納するデータベースを備え、前記通信品質決定手段は、前記データベースを参照し、前記属性情報に基づいて前記コネクション品質情報を決定することを特徴とする。

【0027】請求項7の本発明の通信品質制御装置では、レイヤ3をIPとし、レイヤ4をTCPとし、レイヤ5をHTTPとし、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号、または該プロトコル番号と前記データグラムのTCPプロトコルヘッダ内のポートアドレス、または前記データグラムのIPヘ

ッダの次ヘッダ値、または該次ヘッダ値と前記データグラムのTCPプロトコルヘッダ内のポートアドレスとを検査し、レイヤ5がHTTPであることを認識するとともに受信データグラムのTCPヘッダまたは、TCPヘッダ及びHTTPメッセージに含まれる一つまたは複数の識別情報を検査し、前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする。

【0028】請求項8の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent typeによりデータグラムのメディア属性、HTTPヘッダに含まれるFromフィールドによりデータグラムを送出したユーザの電子メールアドレス、HTTPヘッダに含まれるUser-Agentによりデータグラムを作成したユーザプログラム名及びVersion、HTTPヘッダに含まれるServerによりデータグラムを作成したサーバソフトウェア名及びVersionの少なくとも1を検査することを特徴とする。

【0029】請求項9の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるDateによりデータグラムの作成日時、HTTPヘッダに含まれるAuthorizationによりデータグラムの認証情報、当該認証情報の暗号化方法、HTTPヘッダに含まれるExpiresによりデータグラムの有効日時の少なくとも1を検査することを特徴とする。

【0030】請求項10の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるPragmaによりデータグラムの要求事項、HTTPヘッダに含まれるCache-Controlによりデータグラムのキャッシュ制御情報、HTTPヘッダに含まれるIf-Modified-SinceによりMethodの実行条件、HTTPヘッダに含まれるIf-Unmodified-SinceによりMethodの実行条件、HTTPヘッダに含まれるリクエスト行(Request-Line)内のリクエストURIによりクライアントの要求しているURI、HTTPヘッダに含まれるLast-ModifiedによりHTTPデータの最終更新日時の少なくとも1を検査することを特徴とする。

【0031】請求項11の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるRefererによりHTTPデータの参照元URI(Uniform Resource Identifiers)、HT

10

20

30

40

50



13

TPヘッダに含まれるLocationによりHTTPデータのおかれているURI、HTTPヘッダに含まれるForwardedによりデータグラムの転送先URI及び転送元ドメインネーム、HTTPヘッダに含まれるContent-Baseによりデータグラムのbase URI、HTTPヘッダに含まれるContent-LocationによりHTTPデータの存在するURI、HTTPヘッダに含まれるMethodによりユーザプログラムからのHTTPデータ要求方法の少なくとも1を検査することを特徴とする。

【0032】請求項12の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるMIME-VersionによりデータグラムがMIME (Multi purpose Internet Mail Extensions) のVersion、HTTPヘッダに含まれるAcceptによりユーザプログラムの許可するメディア属性、HTTPヘッダに含まれるAccept-Charsetによりユーザプログラムの許可する文字セット、HTTPヘッダに含まれるAccept-Encodingによりユーザプログラムの許可するデータグラムのコーディング方法、HTTPヘッダに含まれるAccept-Languageによりユーザプログラムの許可するデータグラムの言語、HTTPヘッダに含まれるContent-Encodingによりデータグラムのエンコード方法、HTTPヘッダに含まれるContent-Languageによりデータグラムの言語の少なくとも1を検査することを特徴とする。

【0033】請求項13の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるStatus Codeによりユーザプログラムからの要求に対するサーバの応答内容、HTTPヘッダに含まれるWWW-Authenticateによりサーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authenticateによりプロキシ・サーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authorizationによりデータグラムの認証情報の少なくとも1を検査することを特徴とする。

【0034】請求項14の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるAllowによりHTTPデータの許可するMethod、HTTPヘッダに含まれるAccept-Rangeによりサーバの許可するRange要求方法、HTTPヘッダに含まれるHostによりHTTPデータを要求されるホスト及びそのポート番号、HTTPヘッダに含まれるIf-RangeによりHTTPデータの取得条件、HTTPヘッダに含まれるPublicによりサーバの許可するMethod、HTTPヘッダに含まれるRangeに

(8)

特開2000- 32056

14

よりユーザプログラムの要求しているHTTPデータのRangeの少なくとも1を検査することを特徴とする。

【0035】請求項15の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent-Lengthによりデータグラムのデータ長、HTTPヘッダに含まれるConnectionによりデータグラムのコネクションの状態、HTTPヘッダに含まれるWarningによりユーザプログラムの要求に対するサーバの応答情報、HTTPヘッダに含まれるRetry-Afterにより要求されたHTTPデータを取得可能な日時、HTTPヘッダに含まれるViaによりバケットを中継してきたプロキシサーバまたはゲートウェイのプロトコルVersion及びホスト名及び使用ソフトウェア名、HTTPヘッダに含まれるTransfer-Encodingによりデータグラムのコーディング方法の少なくとも1を検査することを特徴とする。

【0036】請求項16の本発明の通信品質制御装置によれば、レイヤ3をIPとし、レイヤ4をTCPまたはUDP (User Datagram Protocol) として、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号またはIPヘッダの次ヘッダ値を検査し、レイヤ4がTCPまたはUDPであることを認識するとともに、識別情報として受信データのTCPヘッダまたはUDPヘッダに含まれる一つまたは複数の識別情報を検査し、前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする。

【0037】請求項17の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのUDPヘッダに含まれるchecksumフィールドを検査することを特徴とする。

【0038】請求項18の本発明の通信品質制御装置では、レイヤ3をIPとし、レイヤ4をTCPまたはUDPとし、レイヤ5をDNSまたはTFTPまたはSNMPとして、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号、または該プロトコル番号と前記データグラムのTCPまたはUDPプロトコルヘッダ内のポートアドレス、または前記データグラムのIPヘッダの次ヘッダ値、または該ヘッダ値と前記データグラムのTCPまたはUDPプロトコルヘッダ内のポートアドレスを検査し、レイヤ5がDNSまたはTFTPまたはSNMPであることを認識するとともに、識別情報として受信データのDNSメッセージ、TCPまたはU

15

DPヘッダとDNSメッセージ、TFTPメッセージ、UDPヘッダとTFTPメッセージ、SNMPメッセージ、またはUDPヘッダとSNMPメッセージの何れかに含まれる一つまたは複数の識別情報を検査し、前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする。

【0039】請求項19の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのDNSメッセージにquery typeが存在するかどうかを検査することを特徴とする。

【0040】請求項20の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのTFTPメッセージに含まれるopcodeを検査することを特徴とする。

【0041】請求項21の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのSNMPメッセージに含まれるPDUタイプを検査することを特徴とする。

【0042】請求項22の本発明の通信品質制御装置では、レイヤ3をIPとし、レイヤ4をTCPとし、レイヤ5をFTPまたはSMTPまたはとして、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号、または該プロトコル番号と前記データグラムのTCPプロトコルヘッダ内のポートアドレス、または前記データグラムのIPヘッダの次ヘッダ値、または該ヘッダ値と前記データグラムのTCPプロトコルヘッダ内のポートアドレスを検査し、レイヤ5がFTPまたはSMTPであることを認識するとともに、識別情報として受信データのFTP Command、FTP Reply、TCPヘッダとFTP CommandまたはFTP Reply、SMTP Command、SMTP Reply Code、SMTPヘッダ、TCPヘッダとSMTP CommandまたはSMTP Reply CodeまたはSMTPヘッダの何れかに含まれる一つまたは複数の識別情報を検査し、前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする。

【0043】請求項23の本発明の通信品質制御装置では、転送の物理レイヤをATM転送方式とし、コネクション品質に基づきデータグラム転送処理としてATMの各々のコネクション品質に別々のVC (Virtual

(9)

特開2000- 32056

16

Circuit) を割り当ててデータグラムの転送を行ない、各々のVCはコネクション品質に応じた通信品質制御パラメータが設定されていることにより、データグラムから導出されるメディアの属性に応じた転送が行なわれることを特徴とする。

【0044】請求項24の本発明の通信品質制御装置では、前記通信品質決定手段は、前記通信品質に加えて、コネクション設定のためのコネクション設定メッセージに応じてコネクション設定ロバストネスを選択して設定することを特徴とする。

【0045】請求項25の本発明の通信品質制御装置によれば、前記通信品質決定手段は、前記属性情報により、前記コネクションの通信品質として、最適な帯域幅に関する制御パラメータ、最大遅延時間や遅延時間変動量を含む遅延時間に関する最適な制御パラメータ、パッファ量を含むデータ喪失に関する最適な制御パラメータ、最適な課金情報に関する制御パラメータ、最適なセキュリティ品質に関する制御パラメータのうちの少なくとも1の制御パラメータを決定することを特徴とする。

【0046】請求項26の本発明の通信品質制御装置では、前記通信品質決定手段は、前記コネクションの通信品質に基づき、最適なデータグラムの転送先、最適なデータグラムの転送経路の少なくとも一方を決定することを特徴とする。

【0047】請求項27の本発明の通信品質制御装置では、前記通信品質決定手段は、前記コネクションの通信品質に基づいて、必要に応じて専用の物理回線を該コネクションによって使用し、前記データグラムを暗号化または復号化して転送し、データグラム内の不要な情報を削除し、圧縮によりデータグラムのサイズを削減し、データグラムのトンネリングを行なうことを特徴とする。

【0048】請求項28の本発明の通信品質制御装置では、前記通信品質決定手段は、前記属性情報によりコネクションの通信品質としてコネクション設定優先度またはコネクション転送優先度を設定し、該コネクション設定優先度の高いコネクションのコネクション設定処理を優先し、またはコネクション転送優先度の高いコネクションのデータグラムの転送を優先させることを特徴とする。

【0049】

【発明の実施の形態】

【構成の説明】次に、本発明の実施の形態について図面を参照して詳細に説明する。

【0050】図1は本発明の第1の実施の形態を示す通信品質制御装置6のブロック図である。本実施の形態の通信品質制御装置6は、複数のネットワーク終端装置2a、2b、2c、・・・2n及び5a、5b、5c、・・・5nとプロトコル終端装置3a、3b、3c、・・・3n及び4a、4b、4c、4nの組、そして、各々のプロトコル終端装置を接続する通信データグラム転送

50

17

装置1とから構成されている。

【0051】ネットワーク終端装置2a、2b、2c、  
・・・2nは、受信したデータグラムに関してデータネットワークのプロトコルレイヤの終端を行なう。データネットワークのプロトコルレイヤとは、具体的には、MAC層やATM層等である。プロトコル終端装置3aは、ネットワーク終端装置2aより転送されるデータグラムの通信の品質に基づきIP層などのレイヤ3以下を終端する。同様にプロトコル終端装置3b、3c、  
・・・3nは、ネットワーク終端装置2b、2c、  
・・・2nより転送されるデータグラムの通信の品質に基づきIP層などのレイヤ3以下を終端する。

【0052】通信データグラム転送装置1は、プロトコル終端装置3a、3b、3c、  
・・・3nより受信したデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に対応するコネクションの品質情報に従ってプロトコル終端装置4a、4b、4c、  
・・・4nの何れかにデータグラムを転送する。また、通信データグラム転送装置1は、該コネクションの品質情報に従ってデータグラムを送信する通信品質を決定し、該プロトコル終端装置4a、4b、4c、  
・・・4nに対して通知する。

【0053】プロトコル終端装置4aは、通信データグラム転送装置1よりデータグラムとデータグラムを送信する通信品質を受信すると、通知された通信品質に基づきプロトコルレイヤ3以下の設定を行ない、ネットワーク終端装置5aへ転送し、ネットワーク終端装置5aは、該データグラムを外部ネットワークへ転送する。同様に、プロトコル終端装置4b、4c、  
・・・4nは、通信データグラム転送装置1よりデータグラムとデータグラムを送信する通信品質を受信すると、通知された通信品質に基づきプロトコルレイヤ3以下の設定を行ない、ネットワーク終端装置5b、5c、  
・・・5nへ転送し、ネットワーク終端装置5b、5c、  
・・・5nは、該データグラムを外部ネットワークへ転送する。

【0054】通信品質制御装置1は、論理的には、複数のプロトコル終端装置とにより構成されるが、物理的には、各プロトコル終端装置の全て、またはそのいくつかは同一のハードウェアで構成されていても良い。同様に、通信品質制御装置1は、論理的には、複数のネットワーク終端装置とにより構成されるが、物理的には、各ネットワーク終端装置のすべてまたはそのいくつかは同一のハードウェアで構成されていても良い。具体例をあげると、ATMにおける通信では、VP (Virtual Path) 毎に仮想的な宛先とのパスが限られるため、論理的には、それぞれのVPを一つのネットワーク終端装置により終端するが、物理的には一つの物理回線を終端する終端装置が複数のVPを終端している場合が考えられる。

(10)

特開2000- 32056

18

【0055】送信側のプロトコル終端装置3a、3b、3c、  
・・・3nと受信側のプロトコル終端装置4a、4b、4c、  
・・・4nは、論理的には、送信、受信と別の機能を有するが、物理的にはそれぞれが同一のハードウェアで構成されていても良い。同様に、送信側のネットワーク終端装置2a、2b、2c、  
・・・2nと受信側のネットワーク終端装置5a、5b、5c、  
・・・5nは、論理的には、送信、受信と別の機能を有するが、物理的にはそれぞれが同一のハードウェアで構成されていても良い。

【0056】図2は、上記した通信データグラム転送装置1の構成例を示すブロック図である。

【0057】通信データグラム転送装置1は、入力キュー管理部11、出力キュー管理部12、レイヤ識別部13、属性検出部14、通信品質決定部15、経路決定部16、コネクション通信品質管理部17、QOSデータベース150、経路テーブル160、コネクションー通信品質テーブル170より構成される。

【0058】入力キュー管理部11は、各プロトコル終端装置3a、3b、3c、  
・・・3nよりデータグラムが入力されると優先度の高いデータグラムを選択すると共に、該データグラム(D)をレイヤ識別部13と出力キュー管理部12に対して出力する。

【0059】レイヤ識別部13は、図3のフローチャートに基づいて動作する。まず、レイヤ識別部13は、入力された該データグラム(D)に関して、各レイヤの識別を行なう(ステップ301)。具体的には、レイヤ3がIPである場合、IPヘッダのバージョンによりIPプロトコルのバージョンを認識し、レイヤ3がIPv4である場合、IPヘッダのプロトコル番号、または前記プロトコル番号と該データグラムのTCPまたはUDPプロトコルヘッダのポート番号を参照することによりアプリケーションを識別する。また、レイヤ3がIPv6である場合、IPヘッダの次ヘッダ値、または前記次ヘッダ値とTCPまたはUDPプロトコルヘッダのポート番号を参照することによりアプリケーションを識別する。

【0060】レイヤ識別部13は、入力された該データグラム(D)より通信品質を決定するトラフィックの単位となるコネクションの識別を行なう(ステップ302)。具体的には、レイヤ3がIPでありレイヤ4がTCPまたはUDPである場合、IPヘッダの送信IPアドレス、宛先IPアドレスとTCPまたはUDPヘッダの送信ポート番号、宛先ポート番号の組からなるコネクション識別情報によりコネクションを識別する。

【0061】レイヤ識別部13は、前記コネクション識別情報により識別したコネクションにおいて、該コネクションの状態を識別し、コネクション通信品質管理部17に対して、コネクション情報(C)として、コネクションの識別情報とコネクションの状態情報を出力する

19

【ステップ303】。コネクションの状態を識別するには、具体的には、レイヤ4がTCPである場合、TCPヘッダ内部のコードビットにおいて、SYNフラグが立っていることによりTCPのコネクションの確立が行なわれていることを認識し、FINフラグが立っていることにより、TCPのコネクションが終了することを認識する。

【0062】レイヤ識別部13は、経路決定部15に対して、経路を決定するために必要な情報を(A)を出力する(ステップ304)。

【0063】そして、レイヤ識別部13は、前記識別したコネクションの状態をもとに、属性検出部14においてレイヤ4以上の属性を検出する必要があるかどうかを判断する(ステップ305)。

【0064】レイヤ4以上の属性を検出する必要があると判断した場合、属性検出部14に対して、該データグラムの前記レイヤ情報(L)と属性検出部14が各レイヤから属性を検出するために必要なデータグラムの一部分もしくは全部(DP)を出力する(ステップ306)。属性検出部14においてレイヤ4以上の属性を検出する必要がある場合というのは、例えば、HTTPセッションにおいて、セッションの先頭のデータグラムすなわちHTTPヘッダを含むデータグラムを受信した場合である。

【0065】属性検出部14は、レイヤ識別部13から入力される前記レイヤ情報(L)を基に入力されたデータグラムの一部分もしくは全部(DP)から通信の属性情報の検出を行ない、検出された該通信の属性情報(P)を通信品質決定部15へ出力する。

【0066】属性検出部14では、データグラムのレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報の検出を行なうが、コネクションの品質を規定するために必要であれば、レイヤ3以下の情報に関しても検出を行なうものとする。

【0067】通信品質決定部15は、QOSデータベース150を参照し、属性検出部14より入力された通信の属性情報(P)に対応するコネクションの品質情報(S)を検索し、コネクション通信品質管理部17へ出力する。

【0068】経路決定部16は、レイヤ識別部13より入力される前記経路を決定するために必要な情報(A)を基に、経路テーブル160の検索を行ない、データグラムの転送先経路を決定し、コネクション通信品質管理部17へ該データグラムの転送先経路情報(R)を出力する。

【0069】具体的にはレイヤがIPである場合、前記経路を決定するために必要な情報(A)は、宛先IPアドレスであり、宛先IPアドレスをキーとして、宛先IPアドレスの属するIPサブネットワークアドレスまたは宛先IPアドレス自身を検索し、該IPサブネットワ

(11)

特開2000- 32056

20

ークアドレスに対応する次に送信すべき装置のIPアドレスまたはVPI (Virtual Path Identifier) 等を決定する。

【0070】コネクション通信品質管理部17は、図4のフローチャートに基づいて動作する。まず、コネクション通信品質管理部17は、レイヤ識別部13からのコネクション情報(C)及び経路決定部16からの転送先経路情報(R)、または通信品質決定部15からのコネクション品質情報(S)を入力する(ステップ401)。

【0071】コネクション通信品質管理部17は、レイヤ識別部13より入力されるコネクション情報(C)より、コネクションー通信品質テーブル170において管理する必要のあるデータグラム(D)であるかどうか、すなわちコネクションー通信品質テーブルを参照する必要があるデータグラム(D)か、または当該テーブルへの記録の必要があるデータグラム(D)かを判断する(ステップ402)。

【0072】コネクションー通信品質テーブル170において管理する必要のないデータグラム(D)である場合には、レイヤ識別部13より入力されるコネクション情報(C)と経路決定部16より入力される転送先経路情報(R)により、通信品質(Q)を決定し、出力キュー管理部(12)に対して出力する(ステップ403)。

【0073】コネクションー通信品質テーブル170において管理する必要のあるデータグラム(D)である場合、コネクション通信品質管理部17は、コネクションー通信品質テーブル170の検索を行ない、同一のコネクションが存在するかどうかを判別する(ステップ404)。

【0074】コネクションー通信品質テーブル170の検索により同一コネクションが存在する場合は、コネクションー通信品質テーブル170を参照して、通信品質(Q)を設定する(ステップ405)。

【0075】コネクションー通信品質テーブル170の検索により同一コネクションが存在しない場合は、通信品質決定部15から入力されるコネクションの品質情報(S)、レイヤ識別部13より入力されるコネクション情報(C)、経路決定部16より入力される転送先経路情報(R)により、データグラム(D)を転送するための通信品質(Q)を決定し、出力キュー管理部(12)に対して出力する(ステップ406)。その際、コネクション通信品質管理部17は、コネクション情報(C)と通信品質(S)を組にしてコネクションー通信品質テーブル170に記録する(ステップ407)。

【0076】コネクション通信品質管理部17に、通信品質決定部15よりコネクション品質情報(S)が入力されるのは、レイヤ識別部13においてレイヤ4以上の属性を識別する必要があると判断された場合のみであ

10

20

30

40

50

(12)

特開2000- 32056

21

る。コネクション品質情報(S)が入力されない場合には、当該データグラムについてコネクションー通信品質テーブル170による管理を行なう必要がないと判別され、レイヤ識別部13より入力されるコネクション情報(C)と経路決定部16より入力される転送先経路(R2)により、通信品質(Q)を決定する。

【0077】また、コネクション品質情報(S)が入力された場合であっても、当該データグラムについてコネクションー通信品質テーブル170による管理を行なう必要があるかどうかを判別し、レイヤ4以上の参照の必要のないデータグラムに関してはコネクションー通信品質テーブル170による管理を行なわないようにしている。この場合も、レイヤ識別部13より入力されるコネクション情報(C)と経路決定部16より入力される転送先経路(R2)により、通信品質(Q)を決定する。

【0078】HTTPセッションを含むコネクションなどにおいてHTTPヘッダを含むデータグラムを受信した場合など、レイヤ識別部13がレイヤ4以上の属性情報を必要と判断した場合、属性検出部14において検査された属性情報(P)に対応するコネクション品質(S)が通信品質決定部15よりコネクション通信品質管理部17へ入力される。

【0079】コネクション通信品質管理部17は、コネクションー通信品質テーブル170にコネクション情報(C)と通信品質(Q)を組にして記録しておく。一度、コネクション品質(S)に対応する通信品質(Q)が決定すると、レイヤ識別部13より入力されるコネクション情報(C)より同一のコネクションであると認識できるデータグラム(D)は、コネクションー通信品質テーブル170を参照することにより、レイヤ4以上の属性値に対応するコネクション品質(S)に基づく通信品質(Q)が設定され、出力キュー管理部12へ出力される。

【0080】出力キュー管理部12は、入力キュー管理部11より入力されたデータグラム(D)に関して、コネクション通信品質管理部17より入力される通信品質(Q)に基づき、最適なプロトコル終端装置4a、4b、4c、・・・4nを選択し、選択されたプロトコル終端装置に対して、データグラム(D)とデータグラムを送信するために必要な通信品質(Q1、Q2、Q3、・・・Qn)を転送する。

【0081】レイヤ3がIPであり、レイヤ4がTCPであり、レイヤ5がHTTPである場合に関して、本発明の実施の形態における動作に関して説明する。

【0082】コネクション品質情報(S)が入力されない場合とレイヤ4以上のテーブル参照の必要のないデータグラムの場合、デフォルトの動作では、コネクション通信品質管理部17は、コネクション情報(C)と転送先経路(R)よりデータグラム(D)を転送するための通信品質(Q)を決定する。

22

【0083】図5に示すように、HTTPセッション(H0)はいくつかのIPデータグラム(H1、H2、H3・・・)に分割されてネットワーク上を転送されており、HTTPセッションにおいて通信の属性を規定すると考えられるHTTPヘッダを含んだデータグラムは、先頭のデータグラム(H1)である。

【0084】よって、レイヤ識別部13は、TCPヘッダのコードビットを監視することにより、先頭のデータグラム(H1)受信時に、コネクション確立後の最初のデータグラムであることを認識する。そして、レイヤ識別部13は、属性検出部14に対して、レイヤ5がHTTPであるというレイヤ情報(L)を出力する。また、属性検出部14は、データグラム(H1)内のHTTPヘッダより通信品質を決定するために必要な属性を検出し、通信品質決定部15に対して属性情報(P)を出力する。

【0085】通信品質決定部15では、属性検出部14より入力された属性情報(P)を基にQOSデータベース150を検索し、コネクション品質(S)を決定し、コネクション通信品質管理部17に対して出力する。

【0086】コネクション通信品質管理部17は、データグラム(H1)がコネクションー通信品質テーブル170の参照と記録が必要と判断し、通信品質決定部15より入力されたコネクション品質(S)と経路決定部16より入力された転送先経路(R)を基に、データグラム(H1)の通信品質(Q)を決定し出力キュー管理部12へ転送する。

【0087】コネクション通信品質管理部17は、コネクション情報(C)と通信品質(Q)の組をコネクションー通信品質テーブル170に記録する。

【0088】次に、データグラム(H2)を受信した場合、コネクション通信品質管理部17は、レイヤ識別部13より入力されるコネクション情報(C)を基に、コネクションー通信品質テーブルの検索を行ない、データグラム(H1)と同一の通信品質においてデータグラムの転送が行なわれる。

【0089】データグラム(H3)以降においても、同様にデータグラム(H1)と同一の通信品質においてデータグラムの転送が行なわれる。

【0090】本発明の通信データグラム転送装置1は、あくまでもデータグラムのレイヤ3以下を終端しデータグラムの転送を行なうため、既存のルータ装置と同様に高速であるが、必要に応じてレイヤ4以上の通信属性を検査し、該通信属性に対応する最適な通信品質においてデータグラムを転送することが可能である。

【0091】

【実施例1】次に、通信データグラム転送装置1の実施例として、転送の物理レイヤをATM転送方式とし、レイヤ3がIPv4、レイヤ4がTCP、レイヤ5がHTTPであるデータグラムの転送を行なう場合に関して、

50

属性検出部13において検出する属性情報(P)の内容、及び、通信品質決定部14において属性情報(P)より決定するコネクション品質(S)の内容、及び、コネクション品質(S)によりどのような通信品質を提供するかに関して、より具体的に説明する。

【0092】HTTPセッションの最初のデータグラムを受信した際、レイヤ識別部13は、IPヘッダのプロトコル番号が6であることよりレイヤ4がTCPであることを認識し、TCPヘッダのポート番号が80であることよりレイヤ5がHTTPであることを認識し、レイ

ヤ情報として属性検出部14へ出力する。

【0093】属性検出部14は、レイヤ5がHTTPであることから、HTTPヘッダにContent-Type(21)、Server(22)、User-Agent(23)、From(24)が存在するかのチェックを行ない、存在する場合その属性値と共に、通信品質決定部15へ出力する。

【0094】RFC(Request For Comment)1521で規定されているContent-Type(21)は、メディア属性を示し、基本タイプ/サブタイプの組で表現される。例えば、基本タイプが、“image”の場合は画像を、“video”の場合は動画、“audio”の場合は音声、“text”の場合はテキストデータ、applicationの場合はアプリケーションデータであることが分かる。Server(23)は、HTTPによる要求に回答するサーバのプログラム名、バージョンを示す。User-Agent(22)は、HTTPによりデータを要求するユーザの使用クライアントプログラム名、バージョンを示す。From(24)は、HTTPによりデータを要求するユーザの電子メールアドレスを使用する。

【0095】属性検出部14は、コネクション品質を決定するための属性値として、HTTPヘッダから検出する属性値以外に、IPヘッダより宛先IPアドレス(41)、送信元IPアドレス(42)を検出し、通信品質決定部15へ出力する。

【0096】通信品質決定部15は、属性検出部14より入力される各属性値を基に、QOSデータベース150の検索を行なう。本実施例では、QOSデータベース150として、図7の基本QOSテーブル150Aと、図8の拡張QOSテーブル150Bを用いる。

【0097】図7の基本QOSテーブル150Aを参照すると、Content-Type(21)の属性値を基に、遅延優先度(31)、損失優先度(32)、帯域(33)、コネクション優先度(34)が設定されている。

【0098】遅延優先度(31)は、値が大きいものほど優先的に転送されることを意味する。損失優先度(32)は、値が大きいものほどセル損失が低く抑えられる

ことを意味し、値が小さいものは輻輳発生時などに優先的に廃棄される。コネクション優先度(34)は、値が大きいものほど優先的にコネクションを設定することを意味する。

【0099】図7の例では、Content-type(21)の値により、メディア属性が画像であるか、音声であるか、動画であるか、他のデータであるかの判断を行ない、音声や動画の場合には、他のメディアに比べ遅延優先度を高く設定することによりリアルタイムでの通信が可能となるようにしている。また、音声、画像、動画の各メディアは、その他のデータアプリケーションに比べ少々のデータ損失が許されるため、損失優先度(32)が小さく設定されている。

【0100】図8の拡張QOSテーブル150Bの例を参照すると、宛先IP(41)、送信元IP(42)、Content-Type(21)、Server(22)、User-Agent(23)、From(24)を基に、遅延優先度(31)、損失優先度(32)、帯域(33)、コネクション優先度(34)、付加品質(35)、転送先VPI(36-2)を決定する。

【0101】遅延優先度(31)、損失優先度(32)、帯域(33)、コネクション優先度(34)の定義は、前記基本QOSテーブル150Aと同一であるが、その属性値に関しては、基本QOSテーブル150Aで設定された値との差分を設定することができる。例えば、項番(50)が“1”の場合を参照すると、属性検出部14より入力されたServer(22)が“Server1”というプログラム名であった場合、損失優先度(31)は基本QOSテーブル150Aにより規定される値“+1”に設定され、帯域(33)は基本QOSテーブル150Aにより規定される値“+10%”に設定される。

【0102】同様に、User-Agent(23)により規定されるクライアント名や、From(24)で規定されるユーザの電子メールアドレスによって、各コネクション品質(31、32、33、34)を変更することにより、通信品質制御装置を使用するユーザとの契約条件に基づき最適なパラメータを設定することが可能である。項番(50)が“4”の場合、“User2”という電子メールアドレスを持つユーザが“client2”というプログラムを使用して動画通信を行なった場合に、遅延優先度(31)、損失優先度(32)、コネクション優先度(34)が高く設定され、帯域(33)も通常の30%多く設定されるため、より質の高い動画通信を実現可能である。

【0103】項番(50)が“5”の場合、送信元IP(42)がIPアドレス2であるユーザが“Server2”というサーバプログラムと通信を行なう場合に、図8に記されたコネクション品質が設定される。このよ



うに、レイヤ4以上より識別された属性情報だけでなく、必要に応じてレイヤ3以下の属性情報をも利用することによりコネクションの品質を決定する。

【0104】転送先VPI(42)は、データグラムの転送先を決定する。

【0105】基本的に、データグラムの転送先は、経路決定部16において、経路テーブル160を参照することにより決定する。図9に経路テーブル160の例を示す。図9を参照すると、経路テーブル160は、宛先サブネットアドレス(43)と転送先VPI(36-1)の組から構成されている。経路決定部16は、レイヤ識別部13より入力される宛先IPアドレス(41)が経路テーブル160内のどのサブネットアドレス(43)に属するかを検索し、対応する転送先VPI(36-1)を決定する。

【0106】拡張QOSテーブル150Bの項番6では、宛先IPアドレス(41)がIPアドレス1であり、Content-Type(21)がapplication/x-newtypeというあるアプリケーションを使用している場合に、転送先VPI(42)をVPI5に設定する。よって、コネクション通信品質管理部17は、通信品質決定部15より入力されるコネクション品質(S)に転送先VPI(36-2)が設定されている場合は、経路決定部より出力される転送先VPI(36-1)よりも優先する。このように通信品質決定部15においても転送先VPI(36)の決定を可能にし、コネクション通信品質管理部17において、経路決定部16で決定する転送先VPI(36-1)よりも通信品質決定部15で決定する転送先VPI(36-2)を優先する機能を有することにより、使用するアプリケーション種別や、使用するユーザにより転送経路または転送先を変更することが可能である。

【0107】付加品質(35)は、コネクション品質としてセキュリティ品質に応じたデータ転送を確保するためのデータグラムの暗号化方法を規定する。図8の項番7では、IPアドレス4からIPアドレス3へのテキストデータの通信では、L2TP(Layer 2 Tunneling Protocol)を用いてデータグラムの暗号化、及びトンネリングを行なうことを示している。

【0108】図8の拡張QOSテーブル150Bでは送信元IP(42)、宛先IP(41)が記入されたIPアドレスと一致するかを判定することにより、コネクション品質を決定するが、図9の経路テーブルと同様に、IPサブネットアドレスを記入し、送信元IP(42)及び宛先IP(41)がIPサブネットアドレスに属するかどうかを判定することにより、サブネットレベルでコネクションの品質を決定する運用も可能である。

【0109】コネクション通信品質管理部17では、通信品質決定部15から入力されるコネクション品質

(S)である、遅延優先度(31)、損失優先度(32)、帯域(33)、コネクション優先度(34)、付加品質(35)と、転送先VPI(36-2)と、経路決定部16から入力される転送先VPI(36-1)をもとにデータグラムを送信するための通信品質(Q)としてVPIとVCIを決定し、出力キュー管理部12へ出力する。

【0110】そして、出力キュー管理部12では、VPIにより定められるパスとVCIにより定められる品質により最適なプロトコル終端装置を選択しデータグラムを転送する。

【0111】出力キュー管理部12では、遅延優先度(31)の高いデータグラムを優先的に処理する。

【0112】出力キュー管理部12では、損失優先度(32)の高いデータグラムに対して多くのバッファ量を用意することにより、輻輳発生時に損失優先度(32)の低いデータグラムから廃棄されるような制御を行なう。

【0113】コネクション通信品質管理部17では、新たなコネクションを検出した場合、もしくは、コネクションの通信品質が変更された場合、必要に応じて他のATM装置の間にVC(Virtual Circuit)の設定を行なう。コネクション優先度(34)の高いデータグラムは、VC(Virtual Circuit)を割り当てる際に、より優先的にコネクションの設定が行なわれる。

【0114】具体的には、以下のように設定を行なう。

【0115】(1)コネクション優先度(34)の高いデータグラムとコネクション優先度(34)の低いデータグラムの両方のVC設定を行なう必要がある場合、コネクション優先度(34)の高いコネクションのVC設定を先に行なう。

【0116】(2)コネクション優先度(34)の高いデータグラムのVC設定ができない場合、コネクション優先度(34)の低いVCを開放して、コネクション優先度(34)の高いデータグラムのVC設定を行なう。

【0117】(3)VCリソースが少なくなってきた場合には、リソースを使い切る前に、コネクション優先度(34)の低いVCを開放する。

【0118】転送先VPI(36)のうちいくつかのVPIに関しては、専用の物理回線を使いパスを設定することにより、セキュリティ品質を高めることが可能である。例えば、転送先VPI(36-2)のVPI6を専用の物理回線として割り当てることにより、図8の拡張QOSテーブル150Bの項番7において、送信元IP(42)がIPアドレス4で宛先IP(41)がIPアドレス3であり、Content-Type(21)が"text"であるデータに関して、専用の物理回線が割り当てられるため、セキュリティ品質の高いデータグラムの転送が可能である。



(15)

特開2000- 32056

27

【0119】本実施例では、QOSデータベース150として基本QOSテーブル150Aと拡張QOSテーブル150Bを用いて、HTTPヘッダとIPヘッダから複数の属性値を検査し、コネクション品質を決定しているが、基本QOSテーブル150Aのみを使用する運用も考えられる。その場合は、HTTPヘッダ内のContent-Typeのみでコネクション品質が決定される。

【0120】

【実施例2】本発明における通信データグラム転送装置において、課金を行なう場合の例に関して説明する。課金は、コネクション通信品質管理部17においてVCコネクション単位で管理する。課金額は、“トラフィック量×基本課金額”より決定するものとする。また、トラフィック量は、VCコネクション単位での通過するパケット数、もしくは転送ワード数、もしくは転送バイト数、もしくは総ビット数によってカウントされる。基本課金額はVCコネクションのコネクション品質に応じて決定するものとする。

【0121】例えば、設定優先度(31)×重み1+損失率(32)×重み2+帯域(33)×重み3+コネクション優先度(35)×重み4+付加サービス量と設定する。付加サービス量は、例えばコネクションに対してL2TPなどのトンネリングアルゴリズムを適用した場合の追加料金である。

【0122】また、課金の対象となるユーザの限定方法に関して、レイヤ3以下の情報を用いる場合は、送信元IPアドレス、宛先IPアドレス等に限定されるが、レイヤ4以上の情報を用いることにより、例えば、HTTPヘッダの、From、Server、User-Agent、Content-Typeを検査することにより、ユーザ電子メールアドレス、使用するサーバプログラム名、クライアントプログラム名、アプリケーション名等によりユーザ及び団体を特定することができる。

【0123】

【実施例3】属性検出部14において、実施例1にてチェックするHTTPヘッダ以外に、新たにDateフィールドの存在チェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。該Dateフィールドより、データグラムの送信時間が取得される。

【0124】通信品質決定部15では、該Dateフィールドのチェックを行ない、設定されている閾値よりも時間が経過している場合、セル損失優先度を最低の0に設定する、もしくは、即座にデータグラムを廃棄する。

【0125】以上の制御により、データ作成後、時間の経過した価値の低いデータを優先的に廃棄する制御が可能である。

【0126】また、通信品質決定部15で、前記Content-Typeが“audio”または“video”である場合に、該Dateフィールドのチェックを

28

行ない、設定されている閾値よりも時間が経過している場合、セル損失優先度を最低の0に設定する、もしくは、即座にデータグラムを廃棄する制御を行なうことにより、リアルタイムアプリケーションに関して、データ作成後、時間の経過した価値の低いデータを優先的に廃棄する制御が可能である。

【0127】

【実施例4】属性検出部14において、実施例1もしくは実施例3にてチェックするHTTPヘッダ以外に、Authorizationヘッダフィールド、もしくはProxy-Authorizationヘッダフィールドの存在チェックを行ない、存在するかどうかを通信品質決定部15へ出力する。該Authorizationヘッダフィールド、もしくは、Proxy-Authorizationヘッダフィールドより、データグラムが認証情報を含んでいるかが判別できる。

【0128】通信品質決定部15では、Authorizationヘッダフィールド、もしくはProxy-Authorizationヘッダフィールドが存在することを検出した場合、損失優先度(32)を高く設定し、付加品質(34)としてデータグラムを暗号化して転送することを決定することにより、認証情報を含んだデータに関してより信頼性の高い通信を実現することが可能である。

【0129】

【実施例5】実施例4に関して、HTTPヘッダのAuthorizationヘッダフィールドが存在するかどうかを検出するだけでなく、属性値を検査し、適用されている認証情報を暗号化方法を認識することにより、より詳細に設定するコネクション品質を決定することも可能である。

【0130】以下、具体的に説明する。

【0131】通信品質制御部15は、Authorizationヘッダフィールドが入力された場合、Authorizationヘッダフィールド内の認証方法が“Basic”であるかどうかをチェックする。認証方法が“Basic”である場合、他の認証方法に比べてセキュリティが弱いため、損失優先度(32)を高く設定して、付加品質(34)としてデータグラムを暗号化して転送することにより、セキュリティの弱い認証方法である“Basic”を認証情報として含んでいるデータグラムについて、より信頼性の高い通信を実現することが可能である。

【0132】

【実施例6】属性検出部14において、実施例1もしくは実施例3もしくは実施例4にてチェックするHTTPヘッダ以外に、新たにExpiresフィールドの存在チェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。該Expiresフィールドより、データグラムの有効日時を判別できる。

【0133】通信品質決定部15では、該Expiresフィールドのチェックを行ない、現在時刻を経過している場合、セル損失優先度を最低の0に設定する、もしくは、即座にデータグラムを廃棄する。

【0134】以上の制御により、データ作成後、時間の経過した価値の低いデータを優先的に廃棄する制御が可能である。

【0135】

【実施例7】レイヤ3がIPv4、レイヤ4がTCP、レイヤ5がSMTPであるデータグラムが入力された場合の実施例に関して説明する。

【0136】属性検出部14は、レイヤ識別部13の出力よりレイヤ5がSMTPであることを認識し、SMTPのメールヘッダの“From:”フィールドが存在するかのチェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。該“From:”フィールドより、メールの送信ユーザの電子メールアドレスを判別できる。

【0137】QOSデータテーブル150には、契約したユーザに関して、“From:”フィールドに対応する、遅延優先度(31)、損失率(32)、帯域(33)、コネクション優先度(34)、付加品質(35)、転送先VPI(42)等の値が設定されている。

【0138】通信品質決定部15では、QOSデータテーブル150の検索を行ない、該“From:”フィールドのユーザ電子メールアドレスに対応するデータが存在するかどうかのチェックを行ない、存在する場合には設定されたコネクション品質、存在しない場合にはデフォルトのコネクション品質を決定する。

【0139】

【実施例8】レイヤ3がIPv4、レイヤ4がTCP、レイヤ5がFTPであるデータグラムが入力された場合の実施例に関して説明する。

【0140】図6にftpアプリケーションによるファイル取得の例を示す。

【0141】図6の例では、ftpserverというホスト名のFTPサーバに対して、user1というユーザ名のユーザがログインし、“test.dat”というファイルを取得している。先頭の数字と“:”は、行数をあらわすために便宜的につけたものである。

【0142】“——>”で始まる行は、クライアントがサーバに対してFTPリコマンドを転送したことを意味しており、3桁の数字と一文字の空白で始まる行は、クライアントがサーバからFTPリプライを受信したことを意味している。

【0143】“test.dat”というファイルを取得する場合、ユーザが“get test.dat”というコマンドを入力(10行目)すると、クライアントは、サーバに対してまずPORTコマンドを出力(11行目)し、サーバよりPORTコマンド成功のFTPリ

プライを受信(12行目)すると、サーバに対してPETRコマンドを出力(13行目)する。FTPアプリケーションでは制御用のコネクションとデータ用のコネクションは別々に設定される。PORTコマンドはデータ転送に使用するTCPコネクションのクライアント側のIPアドレスとポート番号をサーバに伝えるためのコマンドであり、PETRコマンドは、クライアントがサーバに対してファイルを送信するように要求するためのコマンドである。

【0144】図6の例では、クライアント側のIPアドレスは140.252.13.34であり、ポート番号は1174(4×256+150)である。サーバは、PETRコマンドを受信するとPORTコマンドにより指定されたクライアントホストのポートに対してコネクションを接続し、該コネクションを確立すると、クライアントに対してFTPリプライコード“150”のFTPリプライを送信後、該コネクションを利用して指定されたファイルの転送を行なう。

【0145】属性検出部14は、レイヤ識別部13の出力よりレイヤ5がFTPであることを認識し、データグラムがFTPコマンドであるか、FTPリプライであるかの判別を行ない、コマンドまたはリプライの種別を通信品質決定部15へ出力する。

【0146】通信品質決定部15は、送信元IP(42)によりFTP用の帯域増加サービスに登録しているユーザであるかどうかを判別する。登録ユーザであり、FTPコマンドがPORTコマンドであることを受信すると、PORTコマンドのパラメータである、IPアドレスとポート番号を記録しておく。同一コネクションにおいて、次に、PETRコマンドを受信した場合、記録しておいたIPアドレスとポート番号と現在のコネクションにおける宛先のIPアドレスとポート番号により、サーバからクライアントへのファイル転送に使用されるコネクションをあらかじめ識別することができる。

【0147】以上によって、該サーバからクライアントへのファイル転送に使用されるコネクションの帯域(33)を大きく設定することにより、FTPのファイル転送におけるコネクションに対してのみ効率的に大きな帯域を割り当てることが可能である。

【0148】この際、通信品質決定部15は、ファイル転送に使用されるコネクションを識別するための情報と、該ファイル転送に使用されるコネクションに設定したコネクション品質をコネクション通信品質管理部17へ出力する。

【0149】コネクション通信品質管理部17は、該ファイル転送に使用されるコネクションに関して、入力された該コネクション品質を基に通信品質を決定する。

【0150】

【実施例9】実施例8に関して、データグラムより、ファイル転送に使用されるコネクションが確立したことを

伝えるFTPリプライを検出し、さらに、FTPリプライ内部のリプライコードが“150”であることを検出した際(14行)に、リプライコードに続くデータに記されているデータサイズを識別することにより、ファイルサイズによって設定する帯域を変更するという運用も可能である。

【0151】

【実施例10】属性検出部14において、実施例1にてチェックするHTTPヘッダ以外に、新たにPragmaフィールド、もしくは、Cache-Control

フィールドのチェックを行ない、PragmaフィールドもしくはCache-Controlが存在し、その属性値が“no-cache”である場合、通信品質決定部15へ出力する。

【0152】通信品質決定部15では、特定の宛先IP

アドレス(41-1)で規定されるHTTP Serverへのアクセスに関して、キャッシュが使用可能である場合とキャッシュが使用可能でない場合に別々の経路を設定しておく。

【0153】通信品質決定部15は、データグラム内の宛先IPアドレスが登録されてある宛先IPアドレス(41-1)である場合、“no-cache”であるという情報が入力されているかどうかにより、キャッシュが使用可能であるかの判別を行ない、転送する経路を選択する。

【0154】キャッシュを使用するかしないかにより経路を切り替えることにより、ネットワークを流れるトラフィックを分散し、キャッシュを使用しないコネクションに関しては高速なゲートウェイを通過させるようにする等の制御が可能となる。

【0155】

【実施例11】属性検出部14において、受信データグラムがHTTPリクエストメッセージである場合、Request-line内のRequest-URI、If-Modified-Sinceフィールド、If-Unmodified-Sinceフィールドのチェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。

【0156】本通信データグラム転送装置の提供するサービスとあらかじめ契約しているユーザは、管理しているWWWサーバにおいて、頻繁にIf-Modified-Since、もしくは、If-Unmodified-SinceフィールドによるチェックのありそうなURIとその更新時間を登録しておく。通信品質決定部15において、登録されたURIとその更新時間のテーブルを管理する。

【0157】通信品質決定部15は、Request-URIが登録されているURIと一致し、If-Modified-Sinceフィールド、もしくは、If-Unmodified-Sinceフィールドの属性値

が入力されている場合に、その属性値とテーブルより参照される最終更新時間を比較する。

【0158】If-Modified-Sinceフィールドより取得される日時が該URIの最終更新時間より古い場合、もしくは、If-Unmodified-Sinceフィールドより取得される日時がは、経路決定部により出力されるデータグラム転送先経路(R)へデータグラム(D)を転送する。

【0159】If-Modified-Sinceフィールドにより取得される日時が該URIの最終更新時間より古い場合、データグラムの損失優先度(32)を低く設定する、もしくは、該データグラムを廃棄後、Status Codeが304(not modified)であるHTTPレスポンスメッセージを作成し、送信元IPアドレスに対して転送する。

【0160】If-Unmodified-Sinceフィールドより取得される日時が該URIの最終更新時間より新しい場合、データグラムの損失優先度(32)を低く設定する、もしくは、データグラム廃棄後、Status Codeが412(Precondition Failed)であるHTTPレスポンスメッセージを作成し、送信元IPアドレスに対して転送する。

【0161】以上により、不要なトラフィックをサーバ及びネットワーク内に転送しないようにする事が可能である。

【0162】また、あらかじめURIを登録しておく方法以外にも受信したデータグラム(D)がHTTPレスポンスメッセージであり、該データグラムのHTTPヘッダ内にLast-Modifiedヘッダが存在する場合、URI(U)とLast-Modifiedヘッダより得られる最終更新時間の組を登録する方法も考えられる。該URIは、ユーザ端末からWWWサーバへのHTTPリクエストメッセージ内のRequest-URI、もしくは、Request-URIとHostヘッダより抽出される。HTTPリクエストメッセージとHTTPレスポンスメッセージの対応付けは、HTTPリクエストメッセージもしくはHTTPレスポンスメッセージを構成するデータグラム(D)のコネクション情報(C)より判別される。(リクエストメッセージとレスポンスメッセージ間のコネクションの対応付けに関しては、実施例20を参照のこと)登録するURIは、あらかじめ契約しているユーザのサーバもしくはサーバ内の特定ディレクトリに限定しても良いし、すべてのURIを対象としても良い。

【実施例12】属性検出部14において、受信データグラムがHTTPリクエストメッセージである場合に、実施例1にてチェックするHTTPヘッダ以外に、Request-lineのRequest-URIのチェックを行ない、属性値として読み出されるURIを通信品質決定部15へ出力する。

【0163】属性検出部15では、拡張QOSテーブルにURIの項目を追加する。

【0164】属性検出部15は、属性検出部よりURIが入力されると、拡張QOSテーブルの検索を行ない、テーブル内に入力されたURIが存在する場合、拡張QOSテーブルを参照することにより通信品質(Q)を決定する。URIが一致するかどうかのチェックは、ファイル単位で完全に一致するようにしても良いが、登録する際のURIをDirectory単位にし、属性検出部より入力されるURIが登録URIの文字列を含む場合に一致すると判断しても良い。

【0165】URIに応じて通信品質を決定可能とすることにより、登録ユーザに対して、高度かつ多様な通信サービスを実現可能である。

【0166】属性検出部14においてHTTPヘッダから抽出するURIは、Request-line内のRequest-URI以外に、Refererにより抜き出されるHTTPデータの参照元URI、Locationにより抜き出されるHTTPデータのおかれているURI、Forwardedにより抜き出されるデータグラムの転送先URI、Content-Baseにより抜き出されるデータグラムのbase URI、Content-Locationにより抜き出されるHTTPデータの存在するURIのいずれか、もしくは、全てであってもよい。

【0167】

【実施例13】属性検出部14において、受信データグラムがHTTPリクエストメッセージである場合にMethodの検査を行ない、通信品質決定部15へ出力する。

【0168】通信品質決定部15では、本通信データグラム転送装置から送信元IPアドレス方向に対するコネクションのための通信リソースをあらかじめ割り当てることにより、実際にServer側からHTTPレスポンスメッセージを受信した場合に、既に設定されているコネクション品質によりデータグラムをユーザ側へ転送することが可能である。

【0169】設定するコネクション品質(S)として、MethodがGETもしくはPOSTである場合、帯域(33)を大きく設定する。MethodがGETもしくはPOSTである場合、MethodがHEADである場合に比べ情報量が大きいと考えられるため、帯域を有効に割り当てることが可能である。

【0170】

【実施例14】属性検出部14において、実施例1にてチェックするHTTPヘッダ以外に、新たにMIME-Versionのチェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。通信品質決定部15では、基本QOSテーブルにContent-type(21)に加え、該MIME-Version

nの項目を追加し、MIME-VersionとContent-typeの組によりコネクション品質を決定する。

【0171】

【実施例15】属性検出部14において、受信データグラムがHTTPリクエストメッセージである場合に、Accept, Accept-Charset, Accept-Encoding, Accept-Languageの検査を行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。

【0172】通信品質決定部15では、あらかじめ契約を交わしているユーザの運営するWWWサーバに関してWebサーバのIPアドレス、Web Server対応しているメディア属性(51)、文字セット(52)、符号化方法(53)、言語(54)の情報をサーバ情報管理テーブル(500)に登録しておく。サーバ情報管理テーブル(500)の例を図10に示す。

【0173】通信品質決定部15は、属性検出部14より、Accept, Accept-Charset, Accept-Encoding, Accept-Languageのいずれかもしくは複数が入力されると転送するデータグラム内の宛先IPアドレス(41)がServer情報管理テーブル(500)に存在するかのチェックを行なう。宛先IPアドレス(41)が存在する場合、以下の処理を行なう。

【0174】(1) Acceptの属性値がメディア属性(51)に登録されている属性値と一致するかどうかのチェックを行なう。宛先IPアドレス(41)がIPアドレス3である場合、テキストのメディア属性として、“text/plain”と“text/html”に対応している。Acceptの属性値が“text/plain”、“text/html”以外のテキストのメディア属性である場合、メディア属性(51)が一致していないと判断する。

【0175】宛先IPアドレス(41)がIPアドレス3である場合は、他の画像や音声のメディア属性に関しては特に規定していない。宛先IPアドレス(41)がIPアドレス1、IPアドレス2の場合、サーバ情報管理テーブル(400)のメディア属性(51)は、“-”となっている。この場合、Web Serverの対応しているメディア属性(51)は登録されておらず、Acceptの属性値との比較は行なわない。

【0176】(2) Accept-Charsetのメディア属性値が文字セット(52)と一致するかどうかのチェックを行なう。宛先IPアドレス(41)がIPアドレス1である場合、文字セット(52)として、“ISO-8859-1”のみに対応している。Accept-Charsetの属性値が“ISO-8859-1”以外である場合、文字セット(52)が一致していないと判断する。

(19)

35

【0177】(3) Accept-Encodingの属性値が符号化方法(53)と一致するかどうかのチェックを行なう。宛先IPアドレス(41)がIPアドレス1もしくはIPアドレス2である場合、符号化方法(53)として、“gzip”、“compress”に対応している。Accept-Encodingの属性値が“gzip”、“compress”以外である場合、符号化方法(53)が一致していないと判断する。

【0178】宛先IPアドレス(41)がIPアドレス3である場合、符号化方法(53)は“X”となっている。この場合、Web Serverはどの符号化方法(53)にも対応していないことになり、この場合、Accept-Encoding属性値が何であっても、符号化方法(53)は一致していないと判断する。

【0179】(4) Accept-Languageの属性値が言語(54)と一致するかどうかのチェックを行なう。言語(54)がIPアドレス1である場合、言語(54)として、“en”、“jp”に対応している。Accept-Languageの属性値が“en”、“jp”以外である場合、言語(54)は一致していないと判断される。

【0180】通信品質決定部15が、上記処理において、メディア属性(51)、文字セット(52)、符号化方法(53)、言語(54)のいずれかもしくは複数において、一致しないと判定した場合、該データグラムを廃棄し、Status Codeが406(Not Acceptable)であるHTTPレスポンスメッセージを作成し、送信元IPアドレスに対して転送する。

【0181】実施例15は、WWWサーバ側の対応可能な、メディア属性(51)、文字セット(52)、符号化方法(53)、言語(54)を登録しておき、一致しないメッセージを廃棄する制御であるが、クライアント側の対応可能なメディア属性(51)、文字セット(52)、符号化方法(53)、言語(54)を登録する方法も考えられる。

【0182】その場合、HTTPレスポンスメッセージにおいて、Content-Type内のメディア属性(51)、Content-Encoding内の符号化方法(53)、Content-Language内の言語(54)から検出した属性値が登録されていない場合、該コネクションに属するデータグラムを廃棄する、もしくは、損失率を低く設定することにより、無駄なトラフィックをネットワークに転送しないようにすることが可能である。

【0183】

【実施例16】属性検出部14において、受信データグラムがHTTPレスポンスメッセージである場合、Status Codeのチェックを行ない、その属性値と共に通信品質決定部15へ出力する。

特開2000- 32056

36

【0184】通信品質決定部15は、Status Codeが入力されるとその属性値が200(OK)である場合のみ、帯域(33)を大きく設定する。

【0185】Status Codeが200(OK)である場合のみ、該データグラムで規定されるコネクションにおいて多くのデータグラムが転送されることが予想されるため、効率的に帯域を割り当てることが可能となる。

【0186】

【実施例17】属性検出部14において、受信データグラムがHTTPレスポンスメッセージである場合、HTTPヘッダ内にWWW-Authenticateヘッダが含まれるかどうかのチェックを行ない、通信品質決定部15へ出力する。

【0187】WWW-Authenticateヘッダを含むデータグラムが転送された場合、その後、認証情報を含むデータグラム、もしくは、認証後にWWWサーバから受信したデータグラムが含まれている可能性がある。

【0188】通信品質決定部15は受信データグラム(D-17)がWWW-Authenticateヘッダを含んでいるという情報が入力されると、該データグラム(D-17)に含まれる宛先IPアドレス(41)、送信元IPアドレス(42)より、ユーザ端末とWWWサーバ間のHTMLコネクションに対して、一定期間、損失優先度(32)を高く設定し、付加品質(34)としてデータグラムを暗号化して転送するようにコネクション品質(S)を決定することにより、ユーザ端末とWWWサーバ間のデータグラムに関してより信頼性の高い通信を実現することが可能である。

【0189】

【実施例18】属性検出部14において、受信データグラムがHTTPレスポンスメッセージである場合、HTTPヘッダ内にProxy-Authenticateヘッダが含まれるかどうかのチェックを行ない、通信品質決定部15へ出力する。

【0190】Proxy-Authenticateヘッダを含むデータグラムが転送された場合、その後、認証情報を含むデータグラム、もしくは、認証後にProxyサーバから受信したデータグラムが含まれている可能性がある。

【0191】通信品質決定部15は受信データグラム(D-18)がProxy-Authenticateヘッダを含んでいるという情報が入力されると、該データグラム(D-18)に含まれる宛先IPアドレス(41)、送信元IPアドレス(42)より、ユーザ端末とproxyサーバ間のHTMLコネクションに対して、一定期間、損失優先度(32)を高く設定し、付加品質(34)としてデータグラムを暗号化して転送するようにコネクション品質(S)を決定することにより、ユー

(20)

特開2000- 32056

37

ザ端末とproxyサーバ間のデータグラムに関してより信頼性の高い通信を実現することが可能である。

【0192】

【実施例20】本発明の実施例20の形態について図面を参照して詳細に説明する。

【0193】図11は、本発明の実施例20における通信データグラム転送装置1Aの構成例を示すブロック図である。

【0194】属性検出部14は、受信データグラム

(D) がHTTPリクエストメッセージである場合、HTTPヘッダ内のリクエストURI、もしくは、リクエストURIとHostヘッダフィールドより、アクセスするWWWサーバへのabsolute-URI (70) を抽出し、通信品質決定部15Aへ出力する。

【0195】通信品質決定部15Aは、コネクション識別部13より入力されるコネクション情報(C)と属性検出部14より入力される該URI (70) とを組にしてコネクション情報管理テーブル151に登録する。

【0196】属性検出部14において、受信データグラムがHTTPレスポンスメッセージである場合、HTTPヘッダ内にAllowフィールド、Accept-Rangeフィールド、Content-Baseフィールド、Content-Locationフィールドが存在するかの検査を行ない、存在する場合その属性値と共に通信品質決定部15Aへ出力する。

【0197】通信品質決定部15Aは、HTTPヘッダ内のAllowフィールド、Accept-Rangeフィールドのどちらかもしくは両方が入力された場合、Content-Baseフィールドが入力されたかどうかをチェックし、Content-Baseフィールドが入力されている場合、URIテーブル152に、Content-Baseフィールド内の属性値であるabsolute-URIとAllowフィールド内の許可メソッド(80)、Accept-Rangeフィールド内の許可レンジ(81)を組にして登録する。

【0198】Content-Baseフィールドが入力されていない場合、Content-Locationフィールドが入力されているかどうかをチェックし、Content-Locationフィールドが入力されている場合、URIテーブル152に、Content-Locationフィールド内の属性値であるabsolute-URIとAllowフィールド内の許可メソッド(80)、Accept-Rangeフィールド内の許可レンジ(81)を組にして登録する。

【0199】Content-Locationフィールドが入力されていない場合、コネクション情報管理テーブル151より、コネクション情報(C)に対応するURI (70) を読み出し、URIテーブル152にURI (70) とAllowフィールド内の許可メソッド(80)、Accept-Rangeフィールド内の許

38

可レンジ(81)を組にして登録する。

【0200】属性検出部14は、受信データグラムがHTTPリクエストメッセージである場合、HTTPヘッダ内のメソッド(71)を抽出し、通信品質決定部15Aへ出力する。

【0201】属性検出部14は、受信データグラムがHTTPリクエストメッセージである場合、HTTPヘッダ内のRangeヘッダ、もしくは、If-Rangeヘッダが存在するかのチェックを行ない、存在する場合、Rangeヘッダ、もしくは、If-Rangeヘッダの属性値であるレンジ(72)を抽出し、通信品質決定部15Aへ出力する。

【0202】通信品質決定部15Aは、属性検出部14より前記URI (70) が入力されるとURIテーブル152の検索を行ない、該URIに対する許可メソッド(80)もしくは許可レンジ(81)が登録されていないかを検索する。

【0203】許可メソッド(80)が登録されている場合、属性検出部14より入力されるメソッド(71)との比較を行なう。比較の結果、メソッド(71)が登録されていない場合、データグラム(D)を廃棄する、もしくは、廃棄後、Status Codeが405 (Method Not Allowed) であるHTTPレスポンスメッセージを作成し、送信元IPアドレスに対して転送する。

【0204】許可レンジ(81)が登録されており、属性検出部14よりレンジ(72)が入力された場合、許可レンジ(81)とレンジ(72)の比較を行なう。比較の結果、レンジ(72)による要求方法が許可レンジ(81)に登録されているもので無い場合、付加品質(35)としてデータグラム(D)内に存在するRangeヘッダに関連するヘッダを除去するように設定する。

【0205】出力キュー管理部12においてRangeヘッダに関連するヘッダが除去される。

【0206】除去されるヘッダは、データグラム(D)がRangeヘッダを含む場合は、Rangeヘッダ、If-Unmodified-Sinceヘッダ、If-Matchヘッダであり、データグラム(D)がIf-Rangeヘッダを含む場合は、If-Rangeヘッダのみである。

【0207】

【実施例21】この実施例21の基本的構成については、実施例20と同一である。ただし、URIテーブル152の代わりにWWWサーバテーブル153を使用する。

【0208】属性検出部14において、受信データグラムがHTTPレスポンスメッセージである場合に、HTTPヘッダ内のPublicフィールドの検査を行ない、存在する場合その属性値と共に通信品質決定部15

Aに出力する。

【0209】通信品質決定部15Aは、HTTPヘッダ内のPublicフィールドが入力されると、Content-Baseフィールドの属性値であるURI、もしくは、Content-Locationフィールドの属性値であるURI、もしくは、コネクション情報管理テーブル151より読み出されたURI(70)のいずれかよりWWWサーバのホスト名(700)を抽出し、WWWサーバテーブル153にホスト名(700)とPublicフィールド内の許可メスッド(800)を組にして登録する。

【0210】通信品質決定部15Aは、属性検出部14よりURI(70)が入力されるとWWWサーバテーブル153の検索を行ない、該URI(70)より抽出されるWWWサーバホスト名(700)に対応する許可メスッド(800)が登録されていないかを検索する。

【0211】許可メスッド(800)が登録されている場合、属性検出部14より入力されるメスッド(71)との比較を行なう。比較の結果、メスッド(71)が登録されていない場合、データグラム(D)を廃棄する、もしくは、廃棄後、Status Codeが405(Method Not Allowed)であるHTTPレスポンスメッセージを作成し、送信元IPアドレスに対して転送する。

【0212】

【実施例22】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0213】HTTPレスポンスメッセージにContent-Lengthが含まれていることを検出した場合に、Content-Lengthの長さに応じて、帯域(33)を割り当てる。

【0214】

【実施例23】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0215】HTTPレスポンスメッセージにConnectionが含まれていることを検出した場合に、Connectionの属性値がpersistentである場合に、帯域(33)を大きく割り当てる。

【0216】Connectionの属性値がpersistentである場合、他の属性値である場合に比べ多くのデータグラムが転送されると予想されるため効率的なデータグラム転送が可能である。

【0217】

【実施例24】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0218】HTTPレスポンスメッセージにWarningヘッダが含まれていることを検出した場合に、WarningヘッダのWarn-codeが10(Response is stale)である場合、喪失優先度を低く設定することにより、日時の古いデータ

グラムを優先的に廃棄することが可能である。

【0219】

【実施例25】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0220】HTTPレスポンスメッセージにRetry-Afterヘッダが含まれていることを検出した場合に、Retry-Afterより次に要求したURIにアクセス可能時間を抽出し、URI(70)と該アクセス可能時間を組にしてURIテーブル記録する。

【0221】次に、同一のURI(70)に対してアクセスがあった場合、該URIテーブルより前記アクセス可能時間を読み出し、データグラムを受信した時間よりも先である場合、データグラムを廃棄する。

【0222】データグラムを受信してから実際にWWWサーバにデータグラムが転送されるまでの時間を算出可能である場合は、WWWサーバにデータグラムが転送される時間との比較を行なっても良い。

【0223】

【実施例26】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0224】HTTPヘッダ内にViaヘッダを検出した場合、Viaヘッダ内にあらかじめ登録されてあるホスト名、プログラム名が含まれている場合、テーブルに登録してある通信品質(S)を設定し、データグラムを転送する。

【0225】以上の制御により通過するproxyにおけるホスト名、プログラム名によって契約内容に応じた通信品質を提供することが可能である。

【0226】

【実施例27】属性検出部は、受信データグラム(D)がHTTPレスポンスメッセージであり、あらかじめ登録されてあるユーザ宛のIPアドレスである場合、HTTPヘッダ内のTransfer-Encodingヘッダのチェックを行なう。Transfer-Encodingヘッダが存在しない場合、受信データグラム(D)の属するコネクションに対して付加品質(35)としてデータグラムを暗号化して転送するように設定する。

【0227】以上の制御により、Transfer-Encodingヘッダが存在しない、セキュリティの弱いデータグラムを安全に転送することが可能である。

【0228】

【実施例28】受信データグラムのレイヤ4がTCPである場合、属性検出部14は、TCPヘッダのCode bitであるURG(URGent)をチェックし、通信品質決定部15へ出力する。

【0229】通信品質決定部15は、URGフィールドに1が設定されている場合、緊急セグメントであると判断し、遅延優先度、喪失優先度を高く設定することにより、高速で信頼性の高い通信品質を提供する。



(22)

特開2000- 32056

41

【0230】

【実施例29】受信データグラムのレイヤ4がUDPである場合、属性検出部14は、UDPヘッダのchecksumフィールドを検査し値が0であるかどうかをチェックし、通信品質決定部15へ出力する。

【0231】通信品質決定部15は、checksumフィールドの値が0であることを入力されることにより、該データグラムがチェックサムを利用していないことを認識する。該データグラムの宛先IPアドレス、もしくは、転送元IPアドレスがあらかじめ登録しているユーザのIPアドレスと一致する場合、損失優先度を高く設定し、可能であれば、付加品質としてデータエラーの発生しにくい専用の物理回線を利用するように設定する。

【0232】以上の制御によりチェックサムを使用しないUDP通信においても、契約しているユーザに対しては信頼性の高い通信を提供することが可能である。

【0233】

【実施例30】受信データグラムのレイヤ5がDNSである場合、属性検出部14は、query typeが存在するかのチェックを行ない、query typeが存在する場合通信品質決定部15へ出力する。

【0234】通信品質決定部15は、query typeが入力されると、値が252であるかをチェックする。

【0235】値が252である場合、zone transfer要求であり、他のDNSメッセージに比べ多くのデータグラムが転送されることが予想されるため、帯域(33)を大きく設定する。

【0236】

【実施例31】受信データグラムのレイヤ5がTFTPである場合、属性検出部14は、TFTPメッセージに含まれるopcodeを検査し、通信品質決定部15へ出力する。

【0237】属性検出部14は、UDPヘッダに含まれるUDPLengthの検出を行ない、通信品質決定部15へ出力する。

【0238】通信品質決定部15は、opcodeが入力されると値が3であるかのチェックを行なう。

【0239】opcodeが3であり、かつ、UDPLengthより算出されるTFTPメッセージの長さが512である場合、TFTPによりデータの転送が行なわれていることが判別できるので、帯域(33)を大きく設定する。

【0240】opcodeが3であり、かつ、UDPLengthより算出されるTFTPメッセージの長さが512より小さい場合、TFTPによりデータの転送が完了したことが判別できるので、帯域(33)を小さく設定する。

【0241】以上の制御により、データ転送時のみ帯域

42

を大きく割り当てることができるものである。

【0242】

【実施例32】受信データグラムのレイヤ5がSNMPである場合、属性検出部14は、SNMPメッセージに含まれるPDUタイプを検査し、通信品質決定部15へ出力する。

【0243】通信品質決定部15は、PDUタイプのチェックを行ない、PDUタイプが4である場合、SNMPメッセージがトラップメッセージであることを認識し、該データグラムの遅延優先度(31)を高く設定することにより、トラップメッセージを高速に転送することが可能である。

【0244】

【実施例33】本実施例では、実施例1に加え、通信品質決定部15において決定するコネクション通信品質(S)に、新たにコネクション設定ロバストネス(強度)(37)を追加する。予め契約しているユーザは、3段階のコネクション設定ロバストネス(37)の中から1つを選択して設定することができる。

【0245】コネクション通信品質管理部17では、入力されたコネクション設定ロバストネス(37)に基づき、通信品質制御装置6a、6b、6c、6d間のコネクション(図12)を以下のように設定する。

【0246】(1)コネクション設定ロバストネス=1の場合(図13)、通信品質制御装置6aは、コネクションを設定するために必要な情報を持つコネクション設定メッセージを送信すると同時に、データグラムの転送を開始する。通信品質制御装置6b、6cは、コネクション設定メッセージを受信すると、通信品質制御装置6c、6dに対してコネクション設定メッセージを送信すると同時に、受信したデータグラムを転送する。

【0247】(2)コネクション設定ロバストネス=2の場合(図14)、通信品質制御装置6aは、コネクションを設定するために必要な情報を持つコネクション設定メッセージを送信する。通信品質制御装置6b、6c、6dは、コネクション設定メッセージを受信した場合、予め定められた条件でコネクション設定が可能であれば、送信元の通信品質制御装置6a、6b、6cに対して、ACKメッセージを送信する。通信品質制御装置6b、6cは、ACKメッセージ送信後、コネクション設定メッセージを通信品質制御装置6c、6dに送信する。通信品質制御装置6a、6b、6cは、ACKメッセージを受信後、データグラム転送を開始する。以上により、データグラムは繋接する通信品質制御装置とのコネクションが確立されてから転送される。

【0248】(3)コネクション設定ロバストネス=3の場合(図15)、通信品質制御装置6aは、コネクションを設定するために必要な情報を持つコネクション設定メッセージを送信する。通信品質制御装置6b、6cは、コネクション設定メッセージを受信した場合、予め

定められた条件でコネクション設定が可能であれば、送信先の通信品質制御装置6c、6dに対してコネクション設定メッセージを作成して送信する。通信品質制御装置6dは、コネクション設定メッセージを受信した場合、予め定められた条件でコネクション設定が可能である場合、送信元の通信品質制御装置6cに対してACKメッセージを送信する。通信品質制御装置6c、6bは、ACKメッセージを受信すると通信品質制御装置6b、6aに対してACKメッセージを送信する。通信品質制御装置6aは、ACKメッセージを受信後、データ

10 グラム転送を開始する。以上により、データグラムは通信品質制御装置6a、6b、6c、6d間までのコネクションが完全に確立されてから転送されるため、信頼性の高いデータグラム転送が可能となる。

【0249】以上のように、コネクション設定ロバストネスが大きいほどデータグラムが確実に転送されることが保証される。ユーザは転送するデータグラムの要求品質に合わせてコネクション設定ロバストネスを選択する。

【0250】なお、本発明は上述した実施の形態に限定

20 されるものではなく、その技術思想の範囲内において様々な変形して実施することができる。

【0251】

【発明の効果】以上説明したように本発明の通信品質制御装置によれば、以下に述べるような効果が得られる。

【0252】第1に、通信のメディア属性に応じた通信の品質を決定することができる。その理由は、例えばHTTPヘッダにおけるContent-type等のデータグラムにおけるレイヤ5の部分の属性を抜き出すことにより、画像、音声、動画、アプリケーションといったコネクションの属性を識別でき、それぞれに適したコネクション品質に応じて通信ができるからである。

【0253】第2に、あらかじめ登録してあるユーザに対して高度かつ多様な通信サービスを実現できる。その理由は、例えばHTTPヘッダにおけるServer、User-Agent、FromやSMTPにおけるメールヘッダのFrom行などにより、データグラムを送信した、もしくは、送信先のユーザ名や使用クライアントソフト名、サーバソフト名等を特定することができ、あらかじめ登録しているユーザやソフト製作会社に対して、契約内容に基づくコネクション品質を適用してデータグラムの転送を行なうことができるからである。

【0254】第3に、通信品質に応じた課金量で課金を行なうことができる。その理由は、レイヤ4以上により取得される通信属性に対応するコネクション品質に応じて課金を行なう際のレートもしくは基本料金を決定するからである。

【0255】第4に、データグラムがセキュリティ上非常に重要なデータを含んでいるかどうかを判断し、データグラムに対応するセキュリティ品質に応じたデータ転

送を実現できる。その理由は、例えばHTTPヘッダにおいてAuthorizationヘッダフィールドが存在するかどうかを判断することにより、データグラムが認証情報を含んでいるかどうかを検出することができるからである。

【0256】第5に、データグラムの新規性を判断し、コネクションの品質を決定することができる。その理由は、例えばHTTPヘッダにおけるDateやExpires等のデータグラムの作成日時や有効日時などの情報により、時間の観点からデータグラムの重要性を判別でき、古くなったデータを優先的に廃棄する制御を実現可能であるからである。

【0257】第6に、同一のコネクションで認識できる情報だけでなく、他のコネクションにおいて認識した情報を基にコネクション品質を決定し、最適な通信品質でデータグラムを転送可能である。その理由は、例えばFTPアプリケーションのデータグラムが送受信されている際に、FTPコマンドやFTPリプライの内容を識別することにより、新たにファイル転送を行なうための別のコネクションが設定されたことを識別することができ、ファイル転送時にのみ大きな帯域を割り当てるといった制御が可能だからである。

【図面の簡単な説明】

【図1】 本発明の実施の形態における通信品質制御装置の構成例を示すブロック図である。

【図2】 本発明の実施の形態における通信データグラム転送装置の構成例を示すブロック図である。

【図3】 本発明の実施の形態におけるレイヤ識別部の動作を説明するフローチャートである。

30 【図4】 本発明の実施の形態におけるコネクション通信品質管理部の動作を説明するフローチャートである。

【図5】 HTTPセッションをIPデータグラムに分割化する場合の例を示す図である。

【図6】 FTPによるファイル転送の例を示す図である。

【図7】 QOSデータベース内の基本QOSテーブル例を説明する図である。

【図8】 QOSデータベース内の拡張QOSテーブル例を説明する図である。

40 【図9】 経路テーブルの例を説明する図である。

【図10】 サーバ情報管理テーブルの例を説明する図である。

【図11】 通信データグラム転送装置の他の構成例を説明するブロック図である。

【図12】 通信品質制御装置間のコネクション設定例を説明するブロック図である。

【図13】 通信品質制御装置間のコネクション設定例を説明するブロック図である。

50 【図14】 通信品質制御装置間のコネクション設定例を説明するブロック図である。

(24)

特開2000- 32056

45

46

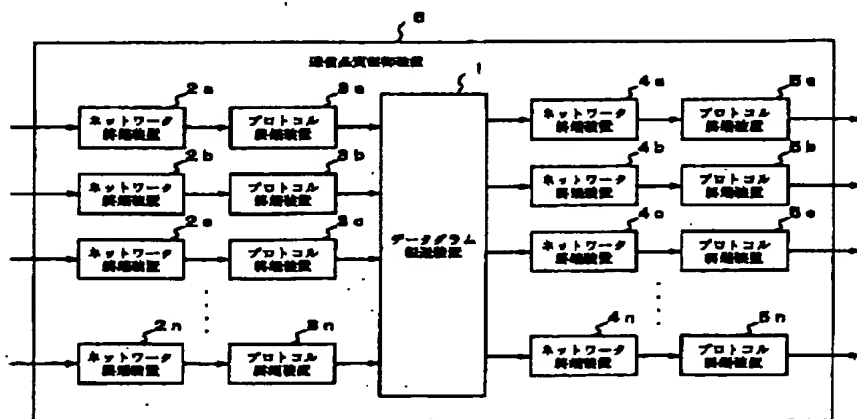
【図15】 通信品質制御装置間のコネクション設定例を説明するブロック図である。

【符号の説明】

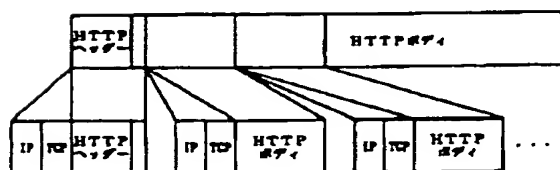
- 1、1A 通信データグラム転送装置  
 2a、2b、2c、・・・2n ネットワーク終端装置  
 5a、5b、5c、・・・5n ネットワーク終端装置  
 3a、3b、3c、・・・3n プロトコル終端装置  
 4a、4b、4c、・・・4n プロトコル終端装置  
 6 通信品質制御装置  
 11 入力キュー管理部  
 12 出力キュー管理部  
 13 レイヤ識別部  
 14 属性検出部  
 15、15A 通信品質決定部  
 16 経路決定部  
 150 QOSデータベース  
 151 コネクション管理テーブル  
 152 URIテーブル  
 160 経路テーブル  
 21 Content-type  
 22 Server  
 23 User-Agent

- 24 From  
 31 遅延優先度  
 32 損失優先度  
 33 帯域  
 34 コネクション優先度  
 35 付加品質  
 36 転送先VPI  
 41 宛先IP  
 42 送信元IP  
 10 43 宛先サブネットアドレス  
 D 転送されるデータグラム  
 C データグラムより検出したコネクション情報  
 A 経路決定部が経路を決定するために必要な情報  
 L データグラムより検出したレイヤ情報  
 DP データグラムの一部もしくは全部  
 P 属性検出部より検査された属性情報  
 S 通信品質決定部において検索されたコネクション情報  
 R データグラムの転送先経路  
 20 Q、Q1、Q2、Q3、Q4 データグラムを転送するための通信品質

【図1】



【図5】

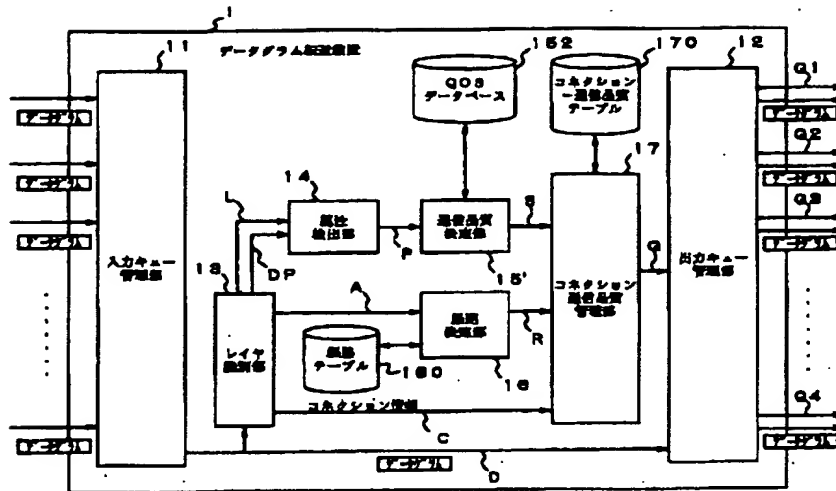


【図7】

経路ロessテーブル

Content-type (21)	遅延優先度 (31)	損失優先度 (32)	帯域 (33)	コネクション 優先度 (34)
image/*	1	2	中	1
audio/*	3	1	小	1
video/*	5	2	大	1
その他	2	3	中	2

【圖 2】



【図6】

【図 9】

```

1:bad! Sftp -d ftopserver
2:Connected to ftopserver.
3:220 ftopserver FTP server (Version 5.0.0 ready).
4:Name (ftopserver:uamr):
5:----> USER uamr!
6:331 Password required for uamr!
7:Password:
8:----> PASS XXXX
9:330 User uamr! logged in.
10:
11:ftp> get test.dat
12:----> PORT 140,223,18,86,4,34
13:200 PORT command successful.
14:----> FEAT test.dat
15:150 Opening BINARY mode data connection for test.dat (38 Kbytes).
16:326 Transfer complete.
17:38 Kbytes received in 0.5 seconds (1 Kbytes/s)
18:ftp>

```

【图 8】

4-9-1257-75

宛先サブネット アドレス (48)	送信先VP I (38-1)
I Pサブネット アドレス1	VP I 1
I Pサブネット アドレス2	VP I 2
I Pサブネット アドレス3	VP I 3
I Pサブネット アドレス4	VP I 4

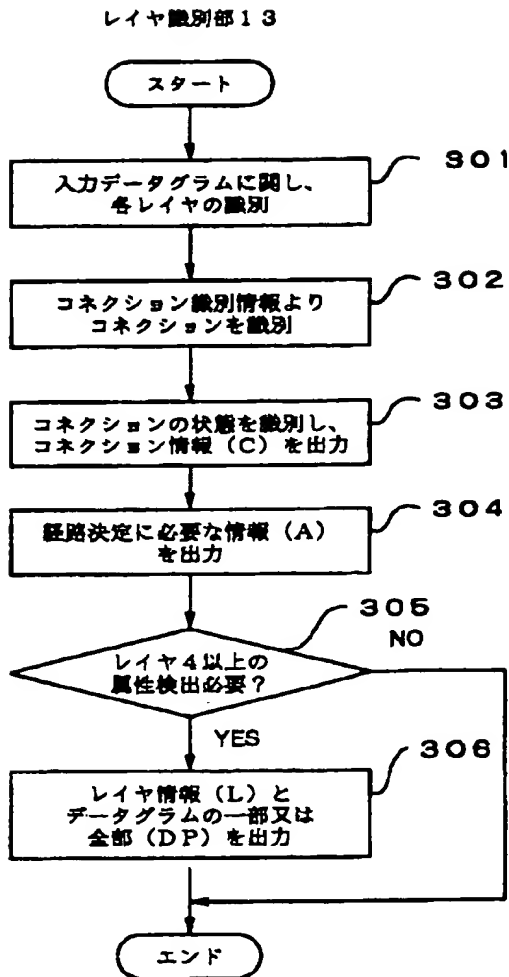
MEMO-74

順序 (50)	映像元IP (42)	映像元IP (41)	Server (38)	User- Agent (35)	From (34)	Content- Type (31)	画面 優先度 (31)	画面 優先度 (33)	帯域 (33)	239767 優先度 (34)	付加品名 (35)	拡張先 VPI Out-IP
1	-	-	Server 1	-	-	-	3	+1	+10%	3	-	-
2	-	-	-	Client 1	-	-	4	+1	+60%	5	-	-
3	-	-	-	-	Door 1	-	+1	3	+60%	4	-	-
4	-	-	-	Client 2	Door 2	video/*	5	4	+60%	4	-	-
5	177.12 8	-	Server 2	-	-	-	3	+1	+10%	3	-	-
6	-	177.12 1	-	-	-	application/ text-type	5	4	大	-	-	1715
7	177.12 9	177.12 9	-	-	-	text/*	5	4	大	4	TCP	1716

(26)

特開2000- 32056

【図3】

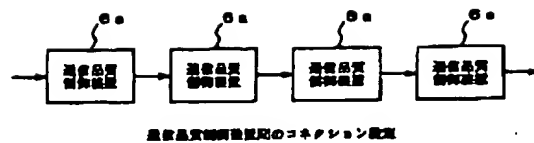


【図10】

IPv4と接続属性テーブル

宛先IP (41)	メディア属性 (51)	文字セット (52)	符号化方法 (53)	言語 (54)
IPアドレス1	-	ISO-10646-1	gzip compress	en_jp
IPアドレス2	-	ISO-10646-1	gzip compress	en
IPアドレス3	text/plain text/html	-	-	en
IPアドレス4	audio/midi image/jpeg	us1code-1-1	-	-

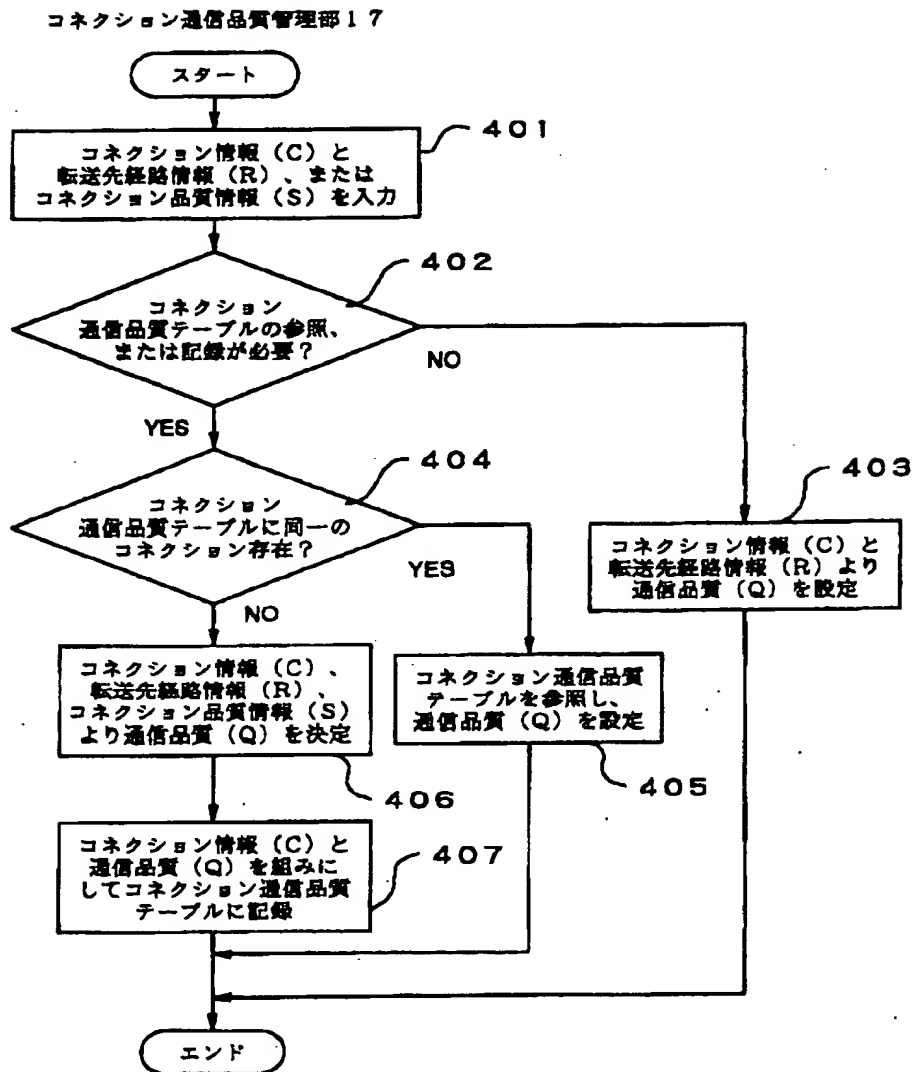
【図12】



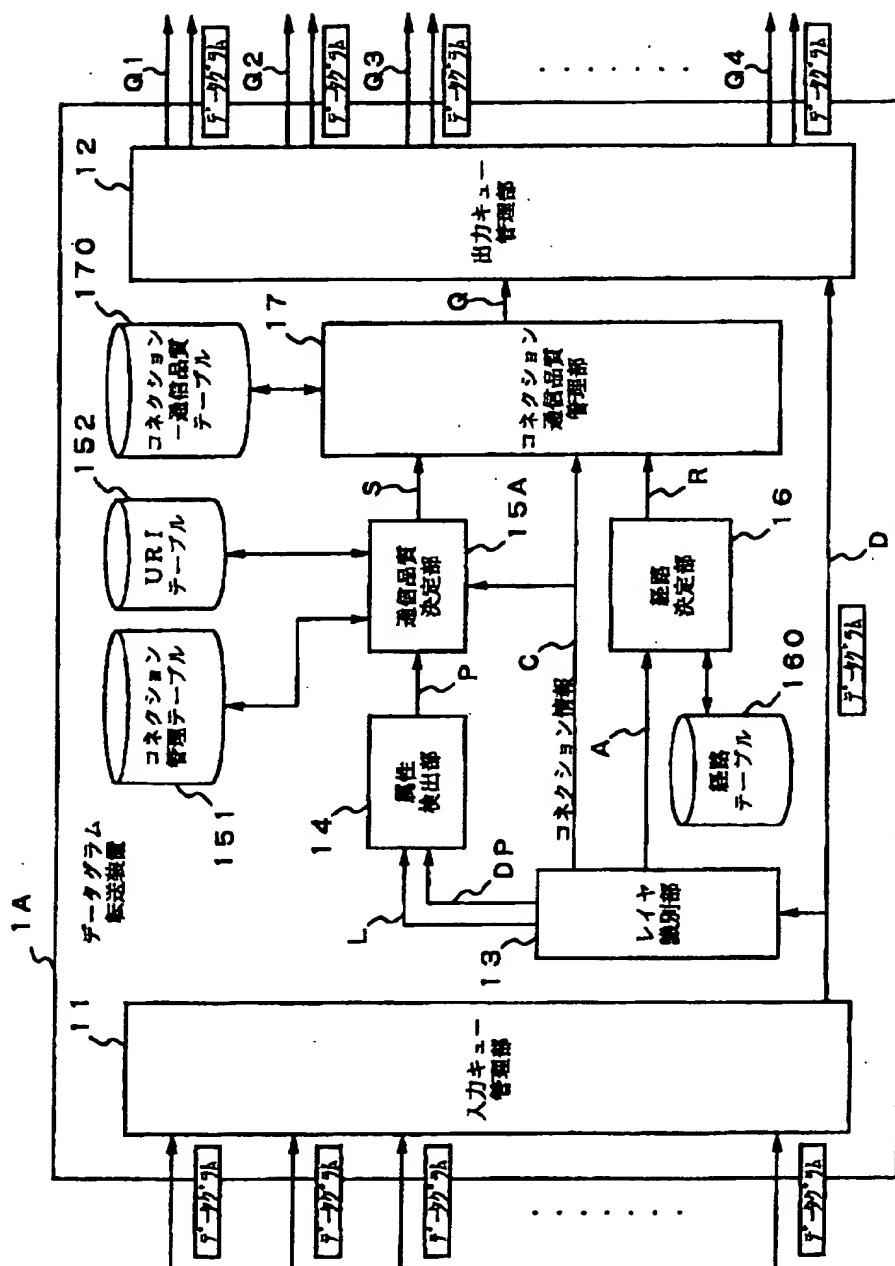
(27)

特開2000- 32056

【図4】



【图 1 1】

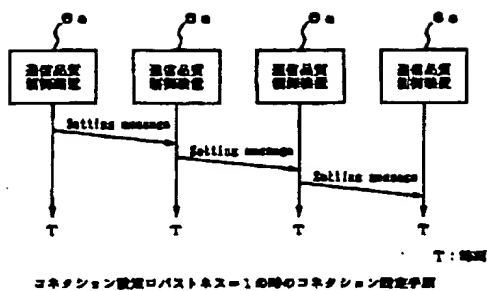




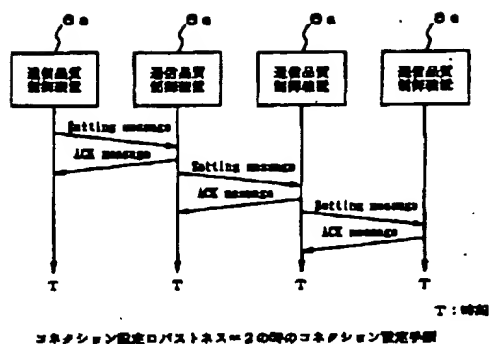
(29)

特開2000- 32056

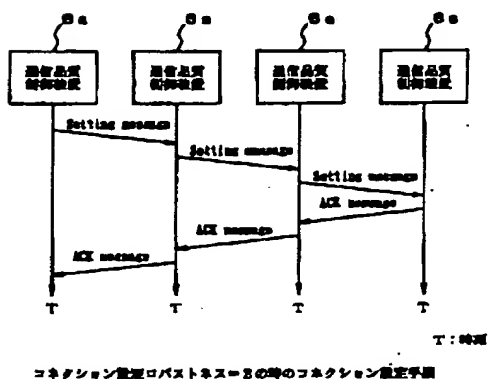
【図13】



【図14】



【図15】



フロントページの続き

(72)発明者 阿留多伎 明良  
東京都港区芝五丁目7番1号 日本電気株  
式会社内

Fターム(参考) 5K030 GA11 GA16 GA19 HA10 HB08  
HB16 HB18 HB21 HC14 HD03  
HD06 JA07 JA08 KA05 KA07  
KA17 KX29 LA03 LB05 LC05  
LC13 LD20  
5K033 AA04 AA08 AA09 BA15 CB01  
CB08 CB17 DA03 DA05 DB16  
DB19